Troubleshooting Routers

Router Software Version 10.0
Site Manager Software Version 4.0

Bay Networks

Bay Networks

4401 Great America Parkway	8 Federal Street
Santa Clara, CA 95054	Billerica, MA 01821

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.

2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.

3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.

4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.

5. Neither title nor ownership to Software passes to licensee.

6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.

8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]

10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.

11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.

12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Chapter 2
Determining the Scope of a Problem

Chapter 3
Troubleshooting an Operational Problem

Chapter 4
Troubleshooting a Physical Media Problem

Chapter 5
Troubleshooting a Data Link Connection Problem

Chapter 6
Troubleshooting a Network Connection Problem

Chapter 7
Troubleshooting a Site Manager Problem

Chapter 8
Getting Help

Index

Figures

Tables

About This Guide

If you are responsible for isolating and solving problems associated with Bay Networks routers, read this guide.

Audience

This guide assumes

- You have experience configuring and managing Bay Networks routers.

- You have a working knowledge of Site Manager and the Technician Interface.

- You have a working knowledge of the protocols running on your routers.

Before You Begin

Before using this guide to solve a problem, refer to the following documents:

- *Release Notes for Router Software Version 10.0*

- *Release Notes for Site Manager Software Version 4.0*

- *Known Anomalies: Router Software 10.0 and Site Manager 4.0*

This manual assumes that you also have access to the following Bay Networks manuals, which are on the CD-ROM:

- *Using Technician Interface Software*

- *Using Technician Interface Scripts*

- *Managing Routers and BNX Platforms*

- *Event Messages for Routers and BNX Platforms*

- The manuals associated with the software you are using

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.

- In Germany, call 0130-37-32.

- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.

- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
arrow character (➜)	Separates menu and option names in instructions. Example: Protocols➜AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points (. . .)	Indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (" ")	Indicate the title of a chapter or section within a book.
screen text	Indicates data that appears on the screen. Example: Set Bay Networks Trap Monitor Filters
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes | nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone: 1-800-845-9523
FAX - U.S./Canada: 1-800-582-8000
FAX - International: 1-916-939-1010

Acronyms

AAL	ATM adaptation layer
ACE	Advanced Communications Engine
AFN	Access Feeder Node
ALC	adaption layer control
ALN	Access Link Node
AMI	alternate mark inversion
AN	Access Node
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Access Stack Node
AT	AppleTalk
ATM	Asynchronous Transfer Mode
B8ZS	binary eight zeros substitution
BCN	Backbone Concentrator Node
BECN	Backward Explicit Congestion Notification
BERT	bit error rate test
BLN	Backbone Link Node
BN	Backbone Node
BOFL	breath of life
BRI	basic rate interface
CD	Carrier Detect
CHAP	Challenge Handshake Authentication Protocol

CID	channel identifier
CN	Concentrator Node
CRC	cyclic redundancy check
CRN	call request number
CSMA/CD	Carrier Sense Multiple Access/ Carrier Detect (Ethernet)
CSU	channel service unit
CTS	clear to send
DCE	data communication equipment
DLCI	data link control identifier
DLSw	Data Link Switch
DOS	Disk Operating System
DP	Data Path
DPRAM	Dual Port RAM
DS	directory service
DS1E1	multichannel T1/E1 driver service
DSAP	destination service access point
DSL	digital subscriber loop
DSR	data set ready
DSU	digital service unit
DTE	data terminal equipment
DTR	data terminal ready
EIA	Electronic Industry Association
ESF	extended super frame
FDDI	Fiber Distributed Data Interface
FDL	Facility Data Link
FECN	Forward Explicit Congestion Notification (FECN)
FN	Feeder Node
FRE	Fast Routing Engine
FRE-2	Fast Routing Engine - 2
FSI	FDDI System Interface
FSM	finite state machine
FTP	File Transfer Protocol
GAME	Gate Access Management Entity

GFWD	GAME forward
GH	Gate Handle
GRPC	GAME RPC
HSSI	High Speed Serial Interface
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
ILACC	Integrated Local Area Communications Controller
IP	Internet Protocol
IPX	Internet Packet Exchange Protocol
ISAP	internal services access point
ISDN	Integrated Services Digital Network
LAN	local area network
LAPB	Link Access Procedure-Balanced
LB	Learning Bridge
LBO	line build out
LCP	Link Control Protocol
LED	light emitting diode
LLC	logical link control
LN	Link Node
LSDB	link state data base
LSP	link state packet
MAC	media access control
NIS	Network Information Services
NVFS	nonvolatile file system
MCT1	multichannel T1
MIB	management information base
MTU	maximum transfer unit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PC	personal computer (also, program counter)
PCAP	Packet Capture utility
PCR	peak cell rate

PDU	protocol data unit
PPP	Point-to-Point Protocol
PROM	programmable, read-only memory chip
PTP	point-to-point (Standard Protocol)
PVC	permanent virtual circuit
QENET	Quad Ethernet Link Module
RAM	random access memory
RI	ring indicator
RIF	routing information field
RIP	Routing Information Protocol
RJ	registered jack
RLSD	received line signal detection
ROM	read only memory
RQ	rate queue
RTM	routing table manager
RPC	remote procedure call
SF	super frame
SAP	Service Advertising Protocol
SAR	segmentation and reassembly
SCR	sustainable cell rate
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPID	Service Profile Identifier
SPEX	Stack Packet Exchange
SPX	Stack Packet Exchange
SQE	signal quality error
SRM	System Resource Module
STM	server table manager
SWSERV	switched access service
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TEI	terminal endpoint identifier
TI_RUI	command line interpreter

TTL	time to live
ULI	upper layer indication
VC	virtual circuit
VCI	virtual channel identifier
VCL	virtual channel link
VME	Versa Module Eurocard
VPI	virtual path identifier
WCLCK	system clock
WINSOCK.DLL	Windows Socket Dynamic Link Library file
ZIP	Zone Information Protocol

Chapter 1
Introduction

This chapter includes the following sections:

- "Preventing Problems"

- "Preparing to Troubleshoot"

- "Documenting Each Step"

- "Performing One Corrective Task at a Time"

Preventing Problems

The following sections offer tips on how to prevent the most common errors that occur:

- "Reading the Release Notes and Relevant Documentation"

- "Minimizing Disruption When Installing New Software"

- "Selecting the Proper Tool for Configuring a Router"

- "Saving Your Configuration Changes"

- "Backing Up Your Files"

- "Maintaining Consistent Files in Multiple Memory Cards"

- "Handling Memory Cards to Prevent Static Damage"

- "Responding to a Failed prom Command"

Reading the Release Notes and Relevant Documentation

The release notes and the manuals that describe how to configure and manage the protocols on your network provide guidelines on how to prevent problems. Read them before installing or upgrading router or Site Manager software.

Minimizing Disruption When Installing New Software

When installing or upgrading software, or using a new feature for the first time, test it at a time or on a node that minimizes disruption to the network. After verifying the change, make the change and verify it on one node at a time in the network. Doing so will help you to isolate and solve any problems that may occur as a result of the change.

Selecting the Proper Tool for Configuring a Router

We recommend that you use the configuration tools as follows:

- Use the Configuration Manager in remote or local mode when you create a new configuration file or make major changes to an existing configuration file.

- Use the Configuration Manager in dynamic mode only to perform minor changes such as change a filter or add a port.

- Use the Technician Interface to issue **set** and **commit** commands to make minor configuration changes only if the Site Manager is unavailable; the Technician Interface does not provide error-checking.

Caution: *Dynamic changes to the router's base records and global parameters can cause an interruption in service. For example, if you change the size of the bridge forwarding table, the router deletes the table and re-creates it, causing a temporary decline in performance. Therefore, you may want to schedule such changes to minimize their impact on your network.*

Saving Your Configuration Changes

The router overwrites the configuration changes in memory when it reboots. If you use either the Configuration Manager in dynamic mode or the Technician Interface **set** and **commit** commands to change the file in memory, you must perform the following procedures if you want to save your changes.

If you use the Configuration Manager in dynamic mode to make changes, select File→Save or File→Save As to copy the configuration from memory to the media; otherwise the changes will be lost after the router reboots.

If you enter the Technician Interface **set** and **commit** commands, you must enter the following command to copy the modified configuration from memory to the media:

save config *<volume>***:***<filename>*

Backing Up Your Files

Store backup copies of the configuration files on the Site Manager workstation. To prevent confusion, use a log to record the location, name, and purpose of each configuration file you back up. Organizing and naming the backup files on the Site Manager workstation will also help you prevent mix-ups.

Caution: *Always back up a file before deleting it. This includes configuration and log files. And always back up the current log file on the Site Manager workstation before clearing it; you may want to refer to it later to troubleshoot a problem.*

Maintaining Consistent Files in Multiple Memory Cards

If the router uses multiple memory cards, make sure that each file is consistent in each memory card designated for storing files of that type. For example, if you make a change to a router software image or configuration file, save the file to each memory card that contains the same files.

To make sure that the files of the same name are consistent on multiple memory cards, display the directory of each card and compare the sizes of each file.

Handling Memory Cards to Prevent Static Damage

Always use an antistatic wrist strap when handling memory cards; static electricity can damage them.

Responding to a Failed prom Command

Caution: *If the Technician Interface* **prom** *command fails, do not reboot. Instead, call the Bay Networks Technical Response Center.*

If you reboot after the prom command fails, a Bay Networks representative must reinsert new PROMs (programmable, read-only memory chips) on the board and rewrite the PROM software to them before the router can recover.

Preparing to Troubleshoot

- • "Getting Acquainted with the Troubleshooting Tools"
- • "Taking a Snapshot of Your Network"

Getting Acquainted with the Troubleshooting Tools

Troubleshooting is much more complicated when you have to solve a problem that requires an urgent solution and at the same time learn the how to use the tools you need to solve the problem. Read this section and familiarize yourself with the tools before you begin troubleshooting. The instructions later in this manual assume you can use the tools identified in this section.

This chapter includes the following sections:

- • "Using the System Log to Display Event Messages"
- • "Displaying and Changing Configuration Settings and Statistics"
- • "Using Ping"
- • "Using Packet Capture"
- • "Using Inbound Telnet to Access the Technician Interface"

Using the System Log to Display Event Messages

The processor running software in each slot maintains its own log file in local memory. Software entities (such as CSMACD and IP) report messages when routine and noteworthy events occur. When you command Site Manager or the Technician Interface to display the messages, the router automatically assembles the messages from all slots into a single file and displays the file. Use the messages in this file to diagnose a problem with a port, slot, router, or protocol.

You can use the Technician Interface **log** command to display the log in the router's memory or the Events Manager tool's File➔Get Current File option to display it. Refer to *Event Messages for Routers and BNX Platforms* for descriptions of the format and meaning of the event messages.

➡ **Note:** *When using the Events Manager tool to display a log, click on the Descending Order option. If you do this, the Events Manager displays the most recent event messages first. If you display a log in ascending order, and the log contains more events than the maximum that the Events Manager can open, it may not be able to display the most recent events.*

When you view a log or save it to a memory card, the router combines log files from each processor into a single file and sorts the events by date and time.

If a fault event message appears in the log, use the procedures in this guide to help you isolate and correct the problem. If you cannot recover from the fault, contact the Bay Networks Technical Response Center for the appropriate action to take.

⬣ **Caution:** *Always save a copy of the entire log to your memory card when a fault appears. The router saves the log to a memory card only when you issue the Technician Interface* **save log** *<filename> command. The format of the log file is binary. If you request help from the Bay Networks Technical Response Center, we may need the binary version of the log file to troubleshoot the problem. Do not delete the log file from the router until you are sure you solved the problem.*

After viewing all event messages that pertain to a specific problem, and before running tests to isolate the problem, you may want to issue the Technician Interface **clearlog** command or select the Events Manager Administration➔Clear log option to remove all events from the event log and start with a clean slate. We recommend that you save the log before you clear it.

If you want to save a log in ASCII format, select the File➔Save Output to Disk option from the Events Manager window.

A processor board keeps its log file even if you reset the slot in which the board is present. The processor will lose the event messages generated in the slot in which the board is present only if one of the following incidents occur:

• You clear the log.

• The router software diagnostic tests run.

• The processor board loses power because you removed it, a fuse blew, or the router lost power.

Filtering Event Messages

You can use the Technician Interface or Events Manager to filter the display of event messages.

Select View➔Filters to display the Events Manager Configuration Filters window. The Filtering Parameters window appears (Figure 1-1).


```
                    Filtering Parameters

  Legend:
     Highlight   Include in display
     Lowlight    Exclude from display


  Severity                Entities
  Fault                   TI
  Warning                 LB
  Information             IP
  Debug                   SNMP
  Trace                   DECnet IV
                          GAME
                          DP
  Slot                    TFTP
  2                       FDDI
  3                       CSMACD
  4                       ACE
  5                       NVFS


     OK        Refresh      Toggle      Cancel
```
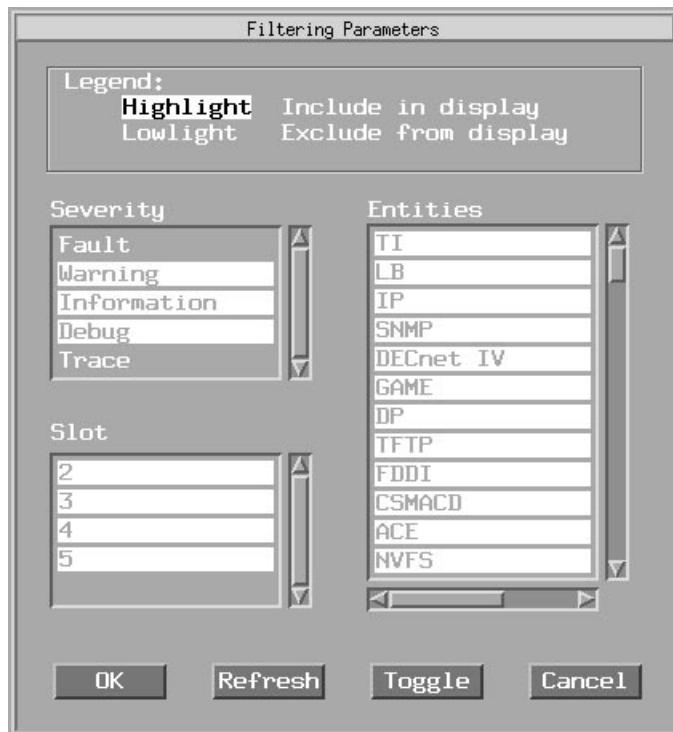
Figure 1-1.   Filtering Parameters Window

The Filtering Parameters window allows you to filter by the severity of the event messages, the software entity reporting them, and the number of the slot from which the entity reported them.

The Technician Interface **log** command supports optional arguments you can use to filter the display of event messages (see Table 1-1).

Table 1-1.   Technician Interface Event Message Filters

To Filter Events By	Use the Following Technician Interface Command Syntax	Technician Interface Example
The software entity (such as IP) that reported the events. **Note**: Always use upper-case letters when specifying a software entity.	**log -e**<*entity*>	l**og -eIP**
The slot number of the processor that reported the events	**log -s**<*slot_no.*>	**log -s3**
The severity of the events. The severities are fault, warning, trace, informational, and debug. When using the Technician Interface to filter events, use the first letter of the severity type.	**log -f**<f | w | t | i | d>	**log -ff**
Starting date and time (supported by the Technician Interface only)	**log -d**<*mm/dd/yy*> **-t**<*hh:mm*>	**log -d01/22/96 -t11:00**

Refer to *Event Messages for Routers and BNX Platforms* for a description of each severity type.

➡ **Note:** *If you Site Manager or the Technician Interface to display the log without filtering explicitly by the severity type, the log displays only fault, warning, and informational events.*

If you are using the Events Manager to view a log and you change the filters, you must refresh or redisplay the event log to use the new filters.

You can specify filters for more than one severity. The Events Manager's Filter window allows you to click on more than one filtering option, and the Technician Interface allows you to enter more than one filter. The following example displays all of the events:

log -ffwtid

You can use the Technician Interface or Events Manager to combine the filters. For example, you enter the following command to display all IP events from 11:19 on 1/22/96:

log -eIP -d01/22/96 -t11:19 -ffwtid

You can filter more than one software entity, slot number, and severity, and combine filter types. The following example filters all severities from Ethernet and IP running on Slots 3 and 4.

log -ffwtid -eCSMACD -eIP -s3 -s4

Refer to the following guides for more detailed information about using the event log:

*   *Managing Routers and BNX Platforms*

*   *Using Technician Interface Software*

*   *Event Messages for Routers and BNX Platforms*

Understanding Debug Messages in the Event Log

One event severity type that raises many questions is Debug. Debug messages help Bay Networks engineers troubleshoot problems. Many Debug messages refer to lines of code and memory addresses that are meaningless to you. The *Event Messages for Routers and BNX Platforms* manual does not describe the Debug messages for this reason.

Note: *Do not become alarmed at Debug messages. They appear routinely in the log. Use the Fault, Warning, Info, and Trace message severities as your primary filters for debugging problems before looking at the Debug messages. By default, Site Manager and the Technician Interface do not display Debug messages unless you use the Debug filter.*

However, displaying the Debug messages can help you to understand the systematic process the software uses to load and initialize discrete software components when starting. And when the software detects a problem, the debug messages can show you the systematic process the software uses to isolate its components, shut them down, and restart them to try to fix the problem.

Many debug messages are meaningless in isolation, but when considered in the context of other messages, they can help you to understand the problem. Debug messages typically contain words such as "creating," "dying," "killing," "gates," and "gate handles."

The name of the router's operating system is GAME (Gate Access Management Entity). In addition to assuming the typical responsibilities of an operating system, GAME creates gates.

Each gate is a process. The process may be to perform a discrete action for a software entity, such as IP. Or it may be to create children gates responsible for their own processes. A parent gate keeps track of its child gate by remembering its logical address, called a gate handle.

If you configure the router to run IP, the gate responsible for creating protocols creates an IP gate. This gate in turn creates gates for IP processes, such as RIP or OSPF. And RIP and OSPF gates create gates of their own to handle RIP and OSPF processes. Thus, each time the operating system starts, it creates gates that form a hierarchy resembling a family tree.

If the software detects a problem, it instructs the parent gate to "kill" (eliminate from memory) the gate associated with the problem, and recreate it. If the problem reoccurs, the software instructs the grandparent gate to kill its children and recreate them. When a gate "dies" (is eliminated), all of its children also die. The grandparent recreates the parent gate, and the parent gate recreates its children. This process expands to the next generation and continues until the problem becomes resolved or until the software entity reinitializes. GAME generates a Fault event message when it reinitializes a software entity. This system of creating and killing gates allows the software to try to correct a problem, but minimizes the impact to the network because it resets only the components that appear to be associated with the problem.

Go to A if you would like to view examples and explanations of Debug messages.

Displaying and Changing Configuration Settings and Statistics

The router's management information base (MIB) determines its configuration and state of operation. The following sections describe how to access the MIB variables:

- "Using the Technician Interface to Access the MIB"

- "Using the Technician Interface Scripts to Access the MIB"

- "Using the Statistics Manager to Access the MIB"

Using the Technician Interface to Access the MIB

The Technician Interface is an out-of-band router management and troubleshooting tool. When the Site Manager connection to the router is unavailable, you can use the Technician Interface as a remote management tool to manage the router and troubleshoot the problem. The *Using the Technician Interface* guide explains how to connect a modem to the router to establish a remote Technician Interface session.

The internal structure of the MIB contains

• Objects. An object is a collection of MIB objects that store data to serve a specialized purpose.

• Attributes. An attribute is a variable (parameter).

• Instances. An instance is a physical manifestation of an attribute.

• Values. A value is the data stored in a location indexed by an object, an attribute associated with that object, and an instance of that attribute.

Suppose you are shopping for a house and a car, and you want to create databases of information about houses and cars on a computer. You create objects (tables) named "House" and "Car" to store this information. You assign each object a unique number called an object identifier. For example, the object identifier for House is 1 and Car is 2. Now you can access information by naming the object or by using its object identifier.

You create attributes to describe houses—attributes such as list price, size of lot, type of house, color, town, street, house number, garage or no garage, number of bedrooms, number of bathrooms, and how much you like it on a scale of 1 to 10. You assign each attribute a unique number called an attribute identifier. For example, you use 1 for list price, 2 for size of lot, 3 for type of house, etc. To access the size of lot, you can specify the object by name ("House") or by identifier ("1"), and the attribute by name ("SizeOfLot") or number ("2") in the format "House.SizeOfLot" or "1.2." Now you can list the attributes of House by entering **list House**.

Example

```
list House
ListPrice = 1
SizeOfLot = 2
TypeOfHouse = 3
Color = 4
```

```
Town = 5
Street = 6
HouseNo = 7
Bedrooms = 8
Bathrooms = 9
TotalSquareFeet = 10
HowMuchILikeIt = 11
```

You set up attributes to describe cars—attributes such as list price, year of manufacture, make, model, automatic or manual transmission, color, number of people it will fit, dealer's name, reputation on a scale of 1 to 10, and how much you like it on a scale of 1 to 10. You assign each attribute a unique number called an attribute identifier. For example, you use 1 for list price, 2 for year of manufacture, 3 for make, etc. To access the attribute reputation, you can specify the object by name ("Car") or by identifier ("2"), and the attribute by name ("Reputation") or number ("8") in the format "Car.Reputation" or "2.8."

Whenever the number of values of an object is limited, you assign code numbers to the values. For example, for the Color attribute of the object House, you use 1 for white, 2 for green, 3 for brown, etc.

Until now, we've been discussing houses and cars in abstractions, not physical manifestations. For example, houses have lot sizes and colors, but a particular house you have seen has a 10,000 square foot lot and is blue. To reference particular houses and cars, you select attributes that, by themselves, uniquely identify them. The town, street, and house number uniquely identify a house, but the town alone or the color does not. The dealer, year, make, and model uniquely identify a car, but the list price alone does not. So you select the format "House.Street.Town" to uniquely identify houses, and the format "Dealer.Year.Make.Model" to uniquely identify cars. The MIB name for a collection of attribute values that you use to identify the physical manifestation of an object is an instance. Thus, House.Street.Town is the instance format of the object House, and 221.Main.Middleton is an instance of that object.

Table shows the object House, its attributes, its instances, and its values. The attributes and instances are in bold, and the values are in regular print.

Table 1-2.   Example of an Imaginary Object Named House

Attributes	Instances		
	221.Main.Middleton	**10.Pleasant.Easton**	**42.Elm.Weston**
ListPrice (1) in thousands of dollars	150	160	170
SizeOfLot (2) in thousands of square feet	10	20	10
TypeOfHouse (3) (1 = colonial, 2 = ranch, 3 = cape)	1	2	1
Color (4) (1 = white, 2 = green, 3 = brown)	2	1	1
Town (5)	Middleton	Easton	Weston
Street (6)	Main	Pleasant	Elm
HouseNo (7)	221	10	42
Garage (8) (0 = none, 1 = one-car, 2 = two-car)	0	1	1
Bedrooms (9)	3	3	2
Bathrooms (10)	1	2	1
TotalSquareFeet (11) (in thousands)	15	18	12
HowMuchILikeIt (12) (1 - 10; 10 is the highest rating)	7	6	3

Suppose you create a lot of diverse objects and you want to organize them. You can create an object to organize and provide access to objects that fit into the same category. For example, you could create an object named ItemsToPurchase and the object identifier 1 to store the objects House and Car. You could group the ItemsToPurchase with an object named Inventory by putting them both in an

object named Things, and assign the object identifier 1 to Things. If you created this hierarchy of objects, you could specify a color of a particular house by connecting the identifier of each object from the top of the hierarchy to the instance. For example, to display the color code of the house at 10 Pleasant St. in Easton, you could enter any one of the following commands:

- **get Things.ItemsToPurchase.House.Color.10.Pleasant.Easton**

- **get House.Color.10.Pleasant.Easton**

  All objects must have unique names. The unique name House provides you with a way to access House without having to specify the objects Things.ItemsToPurchase.

- **get 1.1.1.4.10.Pleasant.Easton**

  In this example, you specify the object identifiers in place of Things.ItemsToPurchase.House.Color.

- **get House.4.10.Pleasant.Easton**

  In this example, you specify the object identifier (4) in place of Color.

The router software uses a large hierarchy of objects that, together, form the MIB (Management Information Base). The software uses the data in these objects to configure itself and to determine its behavior in the network, just as you would have used the data to determine your behavior (that is, select a house and a car).

You can view all the object names in the router's MIB by entering the Technician Interface **list** command. The following example shows a small part of the list of objects you can display with this command. The numbers to the right of the equal sign (=) are not values; they are the numeric identifiers of these objects that you can use in place of the name of the object. When using the Technician Interface, it is easier to enter the object names.

Example

```
list
wfCSMACDEntry = 1.3.6.1.4.1.18.3.4.1.1
wfCSMACDAutoNegEntry = 1.3.6.1.4.1.18.3.4.16.1.1
wfFddiEntry = 1.3.6.1.4.1.18.3.4.4.1
```

When you enter the **list** command, the numbers to the right of the equal sign are the object identifiers, not the values. Dots (.) separate each object. The objects in the example belong to a hierarchy of objects identified by 1.3.6.1.4.1.18.3.4.

You can view all the attribute names and numeric identifiers of an object by entering the Technician Interface **list** *<object>* command.

Example

```
list wfCSMACDEntry
wfCSMACDDelete = 1
wfCSMACDEnable = 2
wfCSMACDState = 3
wfCSMACDSlot = 4
wfCSMACDConnector = 5
wfCSMACDCct = 6
wfCSMACDBofl = 7
wfCSMACDBoflTmo = 8
wfCSMACDMtu = 9
wfCSMACDMadr = 10
```

➡ **Note:** *Do not confuse object or attribute identifiers with values. Identifiers are numbers you can use in place of attribute names.*

For example, the object identifier of wfCSMACDMadr (the media access control address) is 10. When entering the object and attribute in Technician Interface commands to display or change a value, you specify the object by name (wfCSMACDMadr) or object number (1.3.6.1.4.1.18.3.4.1.1) and the attribute by name (wfCSMACDMadr) or number (10). Thus you can specify the object.attribute in any one of the following ways. The first way is the best because you are less likely to make a typing error.

- wfCSMACDEntry.10
- wfCSMACDEntry.wfCSMACDMadr
- 1.3.6.1.4.1.18.3.4.1.1.wfCSMACDMadr
- 1.3.6.1.4.1.18.3.4.1.1.10

➡ **Note:** *The files that describe the MIB are in the* mibs *subdirectory. The default UNIX directory path to the MIB files is* /usr/wf/mibs. *The default DOS directory path to the MIB files is* \wf\mibs. *The files identify and describe each MIB attribute. If the legal values of an attribute are finite, the associated MIB lists them. Use an editor to perform searches of objects that interest you.*

You can view all the instances of an object configured on the router by entering the Technician Interface **list instances** *<object>* command.

➡ **Note:** *Objects, such as wfIpxBase and wfIpBase, that include scalar objects always have the single instance identifier "0."*

Example

```
list instances wfCSMACDEntry
    inst_ids  = 1.1
               1.2
               10.1
               10.2
```

The instance format of the wfCSMACDEntry object is slot.connector. In this example, Connectors 1 and 2 in Slots 1 and 10 are the instances of the wfCSMACDEntry object.

To determine the format of an instance, search for the name of the object in the associated *mibs* file until the specification of the object appears. The "INDEX" field describes the format of the instance associated with that object.

Example

This example shows that the slot and connector form the instance of all attributes of the object named wfCSMACDEntry:

```
wfCSMACDEntry OBJECT-TYPE
        SYNTAX  WfCSMACDEntry
        ACCESS  not-accessible
        STATUS  mandatory
        DESCRIPTION
                " An entry in the csmacd table "
        INDEX   { wfCSMACDSlot,
                wfCSMACDConnector }
        ::= { wfCSMACDTable 1 }
```

Use a period (.) instead of a comma between the elements of an instance. Thus, you express Slot 10, Connector 1 as "10.1" when using the Technician Interface to get or change the values of attributes associated with this instance.

Example

This example shows the instances of the object wfIpInterfaceEntry. The instance format differs from that of the object wfCSMACDEntry.

```
list instances wfIpInterfaceEntry
inst_ids  = 1.1.1.1.100
            1.1.2.1.101
            1.1.3.1.102
            1.1.4.1.103
            1.2.1.1.2
```

The INDEX field in the specification of the object named wfIpInterfaceEntry in the *ip.mib* file shows that the instance format consists of the address of the IP interface and the circuit number:

```
wfIpInterfaceEntry OBJECT-TYPE
    SYNTAX  WfIpInterfaceEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
            " An IP interface description "
    INDEX   { wfIpInterfaceAddr,
            wfIpInterfaceCircuit }
    ::= { wfIpInterfaceTable 1 }
```

You can use the following Technician Interface commands to access the MIB:

- **list** displays the object names and their associated numeric identifiers, as previously described.

- **get** *<object>*.*<attribute>*. *<instance>* displays the value of an object.

- **set** *<object>*.*<attribute>*. *<instance>* *<value>* changes the value of an object.

  You enter **set** commands to make changes to configuration settings. Note the space between the *<instance>* and the *<value>*.

- **commit** changes the value in volatile memory.

  Enter the **commit** command after issuing **set** commands, or they will not work. (When you use the Configuration Manager to make changes and select File➤Save, the router automatically changes the value in volatile memory.)

Remember to save the changes to a file on the router's memory card or floppy disk before rebooting. You can do this with the Configuration Manager or the Technician Interface. When using the Configuration Manager in dynamic mode, select File➤Save. When using the Technician Interface, enter the following command:

save config *<volume>***:***<filename>*

If you do not specify a *<volume>*, the router saves the file to the default volume.

⬡ **Caution:** *The Technician Interface does not perform any error checking when you change the value of a MIB attribute. Whenever possible, use Site Manager to change configuration settings. If you do use the Technician Interface, refer to the appropriate* mib *file to determine which values are legal. Illegal values can disrupt the operation of the router.*

⬡ **Caution:** *Any time you change the setting of a base protocol object, the modified protocol may restart. Consequently, users of the network may lose their connections. If possible, schedule such configuration changes at a time that will minimize network disruption.*

Object and attribute names can be long and are case-sensitive. To reduce errors, we recommend that you use the number of an attribute rather than name it.

When entering a **get** command, you can insert an asterisk (*) in place of an attribute to display all of the attribute values of an instance. For example, the following command displays the value of all of the attributes of the instance 10.1 (Slot 10, Connector 1). (The attributes in this example are a representative sample.)

```
$ get wfCSMACDEntry.*.10.1
wfCSMACDEntry.wfCSMACDDelete.10.1 = 1
wfCSMACDEntry.wfCSMACDEnable.10.1 = 1
wfCSMACDEntry.wfCSMACDState.10.1 = 1
wfCSMACDEntry.wfCSMACDSlot.10.1 = 10
wfCSMACDEntry.wfCSMACDConnector.10.1 = 1
wfCSMACDEntry.wfCSMACDCct.10.1 = 19
```

You can also insert an asterisk in place of the instance in a **get** command to display all of the values of a single attribute. For example, the following command displays the wfCSMACDState of all of the instances. The specification of the wfCSMACDState attribute in the *csmacd.mib* file states "1" means "up" and "2" means "down." Note that you can use this method to display all instances without having to enter the **list instances** *<object>* command.

```
get wfCSMACDEntry.3.*
wfCSMACDEntry.wfCSMACDState.1.1 = 1
wfCSMACDEntry.wfCSMACDState.1.2 = 2
wfCSMACDEntry.wfCSMACDState.10.1 = 1
wfCSMACDEntry.wfCSMACDState.10.2 = 1
```

→ **Note:** *You can use an asterisk in place of the attribute or instance in a* **get** *command, but you cannot use one in place of both.*

You can use the complete MIB number in place of the *<object>*.*<attribute>* specification. The parameter descriptions in the configuration manuals list the MIB number for this reason. SNMP commands also use this syntax.

If you enter a **get** command and the message "object does not exist" appears, do the following:

1. **Check the spelling and case of the object name.**

2. **Configure and enable the object.**

Refer to *Using Technician Interface Software* for more detailed instructions on how to use the Technician Interface to display and change the values in the MIB.

The advantage of using the Technician Interface scripts, the Statistics Manager, or the Configuration Manager instead of the Technician Interface commands is that you don't have to know an object, attribute, and instance in order to display or change a setting. The next two sections introduce you to the Technician Interface scripts and the Statistics Manager. This manual assumes that you already know how to use the Configuration Manager.

Using the Technician Interface Scripts to Access the MIB

The script files are simple programs consisting of one or more SNMP **get** commands that allow you to display menus and values of MIB objects without having to understand the MIB.

To enter script commands, you must do the following:

1. **Use FTP or TFTP to transfer the scripts to a memory card installed in the router.**

2. **Enter the run setpath command to access the *setpath.bat* file to tell the router where to look for the script files.**

You can then enter the **show** or **monitor** script commands with the name of the script menu you want to display. The **show** command displays the statistics at the time you request them. The **monitor** command displays statistics at the time you request them, and continues to refresh the display so that you can see any changes to them.

As you become more proficient with the scripts, you can specify a script file menu option without having to display a menu. For example, the **show at** command displays the AppleTalk script menu, which includes the AARP table option. The **show at aarp** command displays the AARP table.

Refer to *Using Technician Interface Scripts* for detailed instructions on setting up, loading and using the scripts.

Using the Statistics Manager to Access the MIB

The Statistics Manager tools allow you to monitor a router's status and performance from the Site Manager workstation. You can access the statistical values in the MIB by using the following options in the Tools menu of the Statistics Manager window:

• The Quick Get tool allows you to click your way down the MIB tree to a MIB attribute and retrieve its values. Because the Quick Get tool is fast and does not require an initial setup of the screens, this manual refers you to it as an alternative to using the Technician Interface or the scripts.

  The Quick Get tool features a Description button and a Retrieve button.

  If you click an attribute and click Description, a new window displays the description of the attribute from the MIB specification.

If you click an attribute and click Retrieve, the Site Manager retrieves and displays all of the values of that attribute. You can retrieve more than one attribute at a time.

- The Screen Manager tool allows you to select windows of statistics from the Default Screens window, which contains a list of statistics windows provided with Site Manager, and

  — Add them to the Current Screens List window so that you can launch these windows.

  — Copy them to the User Screens window so that you can customize these windows.

- The Launch Facility tool allows you to select from a list of the statistics windows you added to the Current Screens List window to display one.

  When you launch a statistics window, the Statistics Manager queries the router for the values and displays the values.

- The Screen Builder allows you to

  — Build windows of statistics from scratch

  — Customize statistics windows you copied to the User Screens window.

Refer to *Managing Routers and BNX Platforms* for detailed instructions on using the Statistics Manager.

Using Ping

The **ping** command is available both from the Site Manager Administration menu and the Technician Interface. When you enter the ping command, the router, not the Site Manager, issues an ICMP echo request. Options include packet size, number of repetitions, and the capability to trace the path of the ICMP (Internet Control Message Protocol) echo request.

When you lose AppleTalk, APPN, IP, IPX, OSI, or VINES connectivity, use the **ping** command to isolate the problem interface. Try pinging the end node that has connectivity problems. If you fail to get a response, ping the local router interface, and then ping each router interface along the way to the problem node.

If after attempting to ping a device, the response is "Unknown Network" or "Network Unreachable," check the local node's routing table and its default gateway definition.

If the ping command yields the response "Target does not respond," the station you issued the ping from believes it knows how to get to the end node, but never received a reply to its echo request. In this case, start pinging each node in the path between the source and destination until you find the problem interface.

Refer to *Using Technician Interface Software* or *Managing Routers and BNX Platforms* for detailed instructions on issuing a **ping** command.

Using Packet Capture

The Technician Interface Packet Capture tool allows you to filter, send, capture, and view packets in hexadecimal format. You can save the data in a Network General Sniffer format file, transfer the file to a network analyzer, and use the analyzer to parse the data. We recommend that you use Packet Capture to capture data generated at remote routers, save it in Network General Sniffer format files, and use TFTP (Trivial File Transfer Protocol) or FTP (File Transfer Protocol) to transfer the files to a site where you can open the files with a network analyzer.

Appendix B provides detailed instructions on how to use Packet Capture.

Using Inbound Telnet to Access the Technician Interface

Versions 7.60 and higher allow you to use Telnet to establish a Technician Interface session with a router.

➡ **Note:** *We strongly recommend that you learn how to establish an inbound Telnet session with the router in order to troubleshoot problems from a remote site.*

To make Telnet a configurable option in the Protocols menu, create and enable TCP (Transmission Control Protocol) and Telnet Server as follows:

1. **From the Configuration Manager window, select Protocols➤Global Protocols➤TCP➤Create TCP.**

2. **Select Protocols➤Global Protocols➤Telnet Server➤Create Telnet Server.**

   The Telnet Configuration window appears.

3. **Change the settings to the ones you want, or use the default settings, and click OK.**

Unlike the Series 5 software, more than one user can establish an inbound or outbound Telnet session with a router at the same time. However, we do not recommend multiple Telnet sessions because the memory requirements to maintain multiple TCP connections can affect system performance.

For more detailed instructions on how to establish a Telnet connection to a router, refer to *Using Technician Interface Software*.

To troubleshoot Telnet, refer to "Troubleshooting Telnet, FTP, and TFTP" in Chapter 6.

Taking a Snapshot of Your Network

We recommend that you periodically gather and save the forwarding and routing tables maintained by the protocols running in each router. You can use the Technician Interface or the Statistics Manager to do this.

Access to this information will be helpful when you are troubleshooting problems in the future. For example, when troubleshooting a problem, you may find the next hop address to a given destination does not match that in a table you saved previously. This would help you to conclude that there may be a problem with the connection to the node that should be the next hop address.

You can use the Technician Interface to save tables (or any other Technician Interface displays) to a single file as follows:

1. **Access Manager mode.**

2. **Enter the following command:**

    record open *<volume>***:***<filename>*

    <volume> is the number or letter of the router's storage medium you are using to store the file.

    <filename> is the name of the file you are creating to store the text that appears in the Technician Interface.

3. **Display the routing tables.**

4. **Enter the following command to copy the file from memory to the router's file storage medium and terminate the recording:**

    record close

To learn more about the Technician Interface recording feature, enter

help record

You can use the Statistics Manager to save tables to files as follows:

1. **Use the Statistics Manager Screen Manager tool to add the routing tables in the Default Screen List window to the Current Screen List window.**

2. **For each routing table:**

   a. **Use the Launch Facility tool to display it.**

   b. **Use the File➜Save option to save the contents of it to a formatted ASCII file.**

You can use any editor to read the ASCII files, or print and organize them for later reference.

A map of your network configuration is another useful resource to have available for troubleshooting. Include information about the hardware, the software, and the cables you are using. When troubleshooting a problem, compare the next hop on the network map to that of the forwarding table associated with the problem protocol.

Documenting Each Step

An effective troubleshooting strategy includes taking detailed notes as you perform each procedure. These notes are useful because

- They give you an opportunity to pause and think clearly about the problem and the procedures you are following.

  You are more likely to develop a methodical and reasoned approach, and think of solutions during this reflective period.

- They provide you with a record of the tasks you performed. This record is essential because

  — You can refer to it during the procedure in order to recall whether you already performed a certain task.

    A diagnostic procedure can include many tasks. It is easy to forget, for example, which statistics you checked and what they revealed at a given time.

— You can refer to it in order to tell whether, after implementing a test solution, you repeated important diagnostic steps.

— You can refer to notes concerning previous occurrences of the same problem to find hints on how to recover quickly.

— You can provide the information needed by another interested colleague, manager, or Bay Networks Technical Response Center representative if you cannot resolve the problem yourself.

Performing One Corrective Task at a Time

Always perform one corrective task at a time. Then repeat the test that you performed to identify the problem in order to validate the correction. Verify whether the task solved the problem before performing the next corrective task.

This way, you know which task solved the problem. If you perform multiple corrective tasks without verifying the success of each sequentially, you may unknowingly make one of the following mistakes:

- Complicate the original problem.

- Solve the problem but cause another.

- Solve the problem without knowing how you solved it.

Chapter 2
Determining the Scope of a Problem

This chapter poses the initial questions you should answer to narrow the cause of a problem to such topics as router operation, router software, the physical layer, the data link layer, or the network layer. Subsequent chapters provide instructions on how to isolate and solve problems further. The instructions in this chapter tell you which chapters you should go to after determining the scope of a problem.

Determine the scope of a problem by researching and writing down the answers to the following questions:

1. **What are the symptoms of the problem?**

   The more information you have about the symptoms of the problem, the more easily you can identify the cause.

➡ **Note:** *The symptoms of a problem and the underlying cause of the problem are not necessarily the same. For example, if you cannot ping an IP router, the symptom is that you cannot ping the router; the cause may be a loose cable.*

2. **When did each symptom begin?**

   Write down the time you learned about each symptom. Examine the event log for event messages that indicate when the problem occurred. Read the event message descriptions for clues.

3. **What recent changes could have contributed to the problem?**

   - Reconfiguration?

   - Moved nodes?

   - Added segments?

   - Increased traffic?

4. **Are you using a workaround to prevent the symptoms from occurring? If so, what?**

   Consideration of the workaround you are using may help you isolate the problem.

5. **What end stations are involved?**

   Identifying the end stations involved can help you to determine the scope of the problem.

6. **Research and consider the following additional causes:**

   • Traffic congestion

     Examine the statistics and the log to check for traffic congestion. If you determine that traffic congestion is the problem, consider redistributing traffic to relieve the congestion.

   • A software anomaly

     Check the following documents for solutions to your problem:

     — *Release Notes for Router Software Version 10.0*

     — *Release Notes for Site Manager Software Version 4.0*

7. **Look at the LEDs on the router's front and rear panels, and refer to the event log and MIB statistics to answer the following questions.**

   Are the symptoms limited to

   • A single protocol on a single port?

     If so, the problem is most likely in the network layer or above. Refer to Chapter 6.

   • Multiple protocols on a single port?

     If so, the problem is most likely in the physical or data link layer. Refer to Chapters 4 and 5.

   • A single protocol on multiple ports within one slot?

     If so, the problem is most likely in the configuration of the network layer protocol. Refer to Chapter 6.

   • Multiple protocols on multiple ports within one slot?

     If so, and if the same protocols are running OK in other slots, the problem is most likely physical. Refer to Chapter 4.

- A single protocol on multiple ports within all slots running that protocol?

  If so, the problem is most likely in the configuration of the network layer protocol. Make sure you enabled the protocol and refer to Chapter 6.

- Multiple protocols on multiple ports within all slots in the router (box)?

  If so, the problem is most likely operational. Refer to Chapter 3.

- Multiple routers?

  If so, the problem is most likely due to an external device. Try to determine the origin of the problem.

Chapter 3
Troubleshooting an Operational Problem

This chapter describes how to solve problems with the basic operation of the hardware and software. It assumes you have already determined the scope of your problem, as described in Chapter 2.

It includes the following sections:

- "Damaged Router"

- "Power Problem"

- "Blown Fuse"

- "LEDs Not Lit"

- "Router Won't Boot"

- "Checking the Boot PROMs"

- "Making Sure the Router Software Image Is Correct for the Router"

- "Making Sure All Slots Use the Same Router Software Image and Configuration File"

- "Lost Password"

- "No Space Left on Memory Card"

- "Memory or Buffer Problem"

- "Bad Forward Checksum Errors"

- "Fault Message"

Damaged Router

If you detect physical damage to the router, report the problem to the Bay Networks Technical Response Center.

Power Problem

Troubleshoot a power problem as follows:

1. **Make sure the power cable is firmly connected to the router and the electrical outlet.**

2. **Make sure that the Ethernet transceivers have power.**

   If they do not, call the Bay Networks Technical Response Center.

3. **If the router is a BCN® (Backbone Concentrator Node) or CN® (Concentrator Node), determine whether the circuit breaker broke the power circuit.**

4. **If the router is a BCN or BLN® (Backbone Link Node), check the power supply LEDs.**

   If a single power supply LED is off and the power supplies are modular, make sure that the connection is firm. Otherwise, replace the power supply module.

   If more than one power supply LED is off, remove one power supply. If all of the remaining power supply LEDs light, replace the one you removed. Otherwise, reinsert it, and remove another. Repeat this until you find the problem power supply.

Blown Fuse

The following events may cause a fuse to blow:

- A power surge

- You hot-swapped a link module that does not satisfy the minimum version requirements for hot-swap support.

  To determine whether the link module satisfies hot-swap requirements, refer to the *Implementing* guide shipped with the latest upgrade package or to the "Compatibility Matrix" document from the Bay Networks bulletin board, or contact your Bay Networks sales representative.

LEDs Not Lit

The LEDs (light emitting diodes) on a FRE® (Fast Routing Engine), SRM (System Resource Module), or link or net module may fail to light for the following reasons:

- The Ethernet transceivers on a slot lost power.

- A slot is unavailable.

- The backbones are not connected.

- The router blew a fuse.

- The hardware module is not attached firmly to the backplane.

Look at the GAME messages in the event log to determine the cause of the problem. If any of these events occurred and a slot is no longer functional, please call the Bay Networks Technical Response Center to report the problem.

Router Won't Boot

Troubleshoot as follows:

1. **If the router uses a memory card or a diskette, make sure that you inserted it properly. Refer to the appropriate router maintenance guide for instructions.**

➡ **Note:** *If you attempt to boot a router without a storage medium, or attempt to boot a router that does not have the proper router software image and configuration files, it will fail to boot and will stay in the boot mode. The memory cards ship separately; you must install one unless the router is an "Access" product.*

2. **Wait 5 minutes.**

   If the router's file storage mediums do not contain a configuration file named *config*, the router boots automatically with the *ti.cfg* file after five minutes. The *ti.cfg* file contains the minimum configuration required to boot the router and allow you to use the Technician Interface to access it. Make sure you name the configuration file *config*; then reboot the router.

3. **If you recently installed the router software image, make sure it is correct for the router type and media (memory card or diskette) with which you are booting.**

For detailed instructions on router software image compatibility, refer to the *Upgrading Routers from Version 5 to Version 10.0* guide.

4. **If you set up the network to allow the router to netboot, refer to** *Connecting BayStack AN and ANH Systems to a Network* **or** *Connecting ASN Routers and BNX Platforms to a Network***.**

5. **If the router is an ASN**™**, refer to Tables 3-1, 3-1, and the instructions that follow. Otherwise, refer to the LED section of the hardware manual associated with the router to diagnose the problem.**

Table 3-1.   ASN Front-Panel LEDs

Run LED	Diagnostic LED	Meaning
on	off	Normal operation
flashing	flashing (alternately)	SPX failure
flashing	on	Diagnostic failure
flashing	off	Router booting

Table 3-2.   ASN SPX Rear-Panel LEDs

LED	Module	Meaning When On
FR	SPX (Stack Packet Exchange)	SPX transmitting
FC	SPX	Flow control on to reduce data congestion in the backplane

Troubleshoot an ASN as follows:

    a.   **If the ASN is in a stack, make sure the SPX slot dial on the rear panel of each ASN points to a different slot ID. Turn the selector in either direction so that the arrow on the selector points to the ID you want to use ([Figure 3-1](#)). Make sure the configuration matches the slot dial setting.**
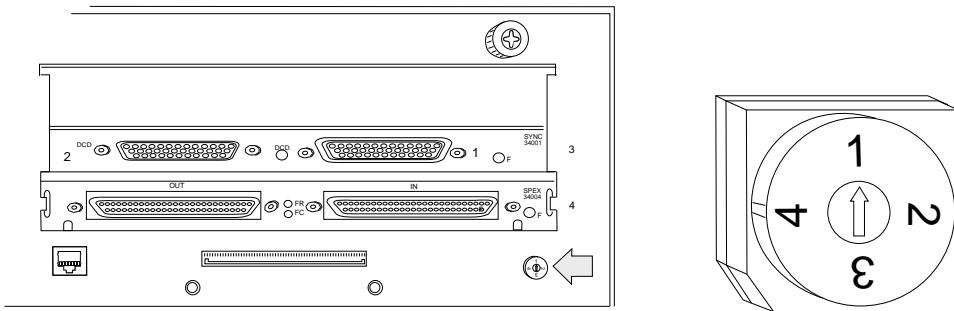
Figure 3-1.   Verifying the Slot ID on an ASN

    b.   **If the SPEX® Net Module does not support hot-swap, make sure that a terminator plug connects to any unused ports labeled SPEX IN and SPEX OUT. Make sure the thumbscrews on the terminator plug are tight.**

If the ASNs are in a stack and they do not support hot-swap, you must terminate the SPEX IN port of the first ASN and the SPEX OUT port of the last ASN. Make sure that for the remaining ASNs in the stack, the SPEX OUT port of one ASN connects to the SPEX IN of the next.

→   **Note:** *The ASN cables are long enough to skip one ASN in the stack for troubleshooting purposes.*

Checking the Boot PROMs

Make sure that the boot PROM images are compatible with the router software image as follows:

Check the boot PROMs as follows:

1. **Enter the following command to display the software version of each boot PROM:**

   get wfHwEntry.19.*

   The slot number containing the boot PROM follows the dot (.) after the "wfHwEntry.wfHwBootPromSource" object name.

   ### *Example*

   ```
   $ get wfHwEntry.19.*
   wfHwEntry.wfHwBootPromSource.2 = "int/8.10/40/freboot.exe"
   wfHwEntry.wfHwBootPromSource.3 = "int/8.10/40/freboot.exe"
   wfHwEntry.wfHwBootPromSource.4 = "int/8.10/40/freboot.exe"
   wfHwEntry.wfHwBootPromSource.5 = "int/8.10/40/freboot.exe"
   ```

2. **Refer to** *Upgrading Routers from Version 5 to Version 10.0* **to make sure the boot PROM versions satisfy the software version requirements.**

Making Sure the Router Software Image Is Correct for the Router

Make sure that the router software image on the router is compatible with the type of router you are using. Refer to the *Upgrading Routers* book that applies to your router software for a list of the router software image names and the associated router types.

Making Sure All Slots Use the Same Router Software Image and Configuration File

Different versions of router software image and configuration files within a router can cause many types of serious problems. The best way to avoid these problems is to maintain consistency among the router software images in multiple memory cards, and make sure that, if you make a configuration change to a configuration file on one memory card, that you copy the file to any other memory cards that have a file with the same name.

However, if you specify the router software image and configuration files when booting the router, all processors boot with the specified router software image and configuration file.

If the router has more than one memory card, refer to the following sections to make sure the router software image and configuration files in each processor are the same:

- "Verifying That the Router Software Images in Each Processor Match"
- "Verifying That the Configuration Files in Each Processor Match"

Verifying That the Router Software Images in Each Processor Match

To display the source of the router software images active in each processor, enter the Technician Interface **get wfHwEntry.28.*** command, or use the Statistics Quick Get tool to display the
wfHardwareConfig➜wfHwTable➜wfHwActiveImageName values.

Example:

```
                              Slot                                Name of
                           location of          Source        image on the
                            processor        volume of            source
                            in router      image in use           volume
$ get wfHwEntry.28.*
wfHwEntry.wfHwActiveImageName.1 = (nil)
wfHwEntry.wfHwActiveImageName.2 = "2:bn.exe"
wfHwEntry.wfHwActiveImageName.3 = "2:bn.exe"
wfHwEntry.wfHwActiveImageName.4 = "2:bn.exe"
wfHwEntry.wfHwActiveImageName.5 = "2:bn.exe"

                                             All settings for
                                             all processors
                                             must be the
                                             same.
```

In this example, the processors in Slots 2 through 5 are operating with the router software image named *bn.exe*, which came from the file system in Volume 2. Here, Slot 1 does not have a configuration because it does not contain a processor module.

If the slots are operating with router software images from different volumes, do the following:

1. **Display the directory for each slot and compare the file sizes of the router software images.**

   If they are the same size, assume that the router software images are consistent and go to the next section, "Verifying That the Configuration Files in Each Processor Match."

2. **Compare the file sizes with the backup router software image stored on the Site Manager workstation.**

3. **Determine which router software image is the one you want to use.**

   If you are not sure about the integrity of any of the router software images on the router or Site Manager, do the following:

   a. **Use the Image Builder to customize an image.**

   b. **Back up the images on the memory cards.**

   c. **Remove the images from the memory cards.**

   d. **Compact the memory cards.**

⬟ **Caution:** *Do not interrupt the compaction.*

   e. **Transfer the image you customized to the memory cards that you want to use to store the image.**

   f. **Reboot the router.**

   g. **If this resolves the problem, stop here. If this does not resolve the problem, go to the next section, "Verifying That the Configuration Files in Each Processor Match."**

4. **Back up the unwanted router software image.**

5. **Remove the unwanted image from the router's file system.**

6. **Determine which slots are running with the incorrect image and reset them.**

Verifying That the Configuration Files in Each Processor Match

To display the source of the configuration files that are active in each processor, enter the Technician Interface **get wfHwEntry.26.*** command. Or use the Statistics Quick Get tool to display the wfHardwareConfig→wfHwTable→wfHwConfigFile values.

Example:

```
                         Slot          Source        Name of
                       location of    volume of    configuration
                       processor    configuration   file on the
                        in router     file in use   source
                                                     volume

$ get wfHwEntry.26.*
wfHwEntry.wfHwConfigFile.1 = (nil)
wfHwEntry.wfHwConfigFile.2 = "2:config"
wfHwEntry.wfHwConfigFile.3 = "2:config"
wfHwEntry.wfHwConfigFile.4 = "2:config"
wfHwEntry.wfHwConfigFile.5 = "2:config"

                                     All settings for
                                     all processors
                                     must be the
                                     same.
```
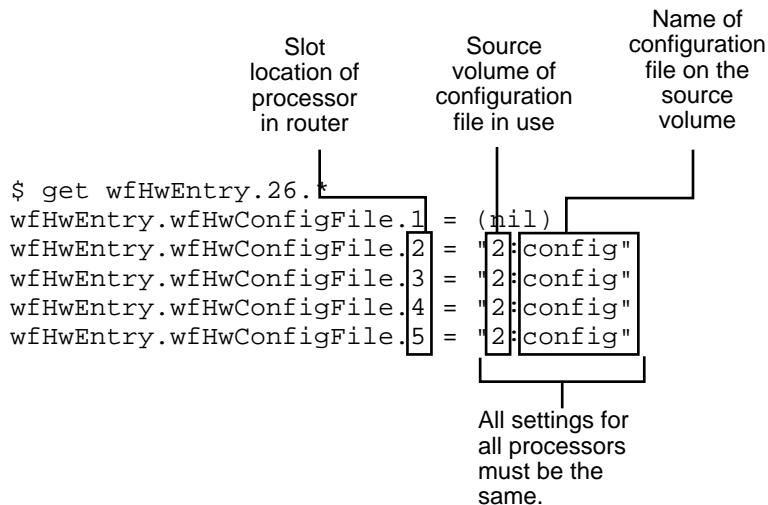
In this example, the processors in Slots 2 through 5 are operating with the configuration file named *config*, which came from the file system in Volume 2.

→ **Note:** *It is OK to use a router software image from one volume and a configuration from another.*

If the slots are operating with configuration files from different volumes, do the following:

1. **Display the directory for each slot and compare the file sizes of the configuration files.**

   If they are the same size, the configuration files are consistent. If they are not, continue with the remaining steps.

2. **Compare the file sizes with the backup configuration file stored on the Site Manager.**

3. **Determine which configuration file is the one you want to use.**

4. **Back up the unwanted configuration file.**

5. **Remove the unwanted configuration file.**

6. **Determine which slots are running with the incorrect configuration file and reset them.**

Lost Password

Danger: *Follow these instructions only if the router you are using is user-serviceable. Routers that are not user-serviceable, such as the AN™, ASN, ANH™, FN™, LN®, CN, and AFN®, can cause electric shock. Call the Bay Networks Technical Response Center if you lost a password in one of these types of routers.*

When you create or change a password, the router distributes it to each FRE processor module, which in turn stores the new password on the local ROM (read only memory) chip. If you remember the old password and want to change it, or you want to add password security for the first time, refer to the "System Administration" chapter in *Using Technician Interface Software* for instructions.

To replace a lost password, you need a FRE module that never operated in a router requiring a password, or one that operated in a router for which you know the password. Replace a lost password as follows:

1. **Disengage the thumb clips that secure all FRE processor modules to the slots and pull each module slightly to disconnect it from the backplane. *Never* completely remove more than one processor module from its slot.**

Danger: *Never operate a router with more than one processor module completely removed from its slot.*

2. **Remove one processor module from its slot.**

3. **Insert a FRE processor module that has never operated in a router that required a password, or one that operated in a router for which you know the password.**

4. **Insert the memory card containing the router software image and configuration file into the FRE processor module.**

5. **Boot the router.**

6. **Engage the thumb clips of the other FRE processor modules.**

7. **Wait for the modules to reset.**

8. **Enter the Technician Interface password** *[Manager | User]* **command to create or change the password.**

   The new FRE processor distributes the new password to the other processors, which then overwrite the old password.

No Space Left on Memory Card

When you delete a file on a memory card, the file system makes the file inaccessible, but the file continues to use space on the card. Each time you store a file, the file system stores the file at the first unused space. Eventually, after you store and delete multiple files, the card runs out of usable space because the deleted files continue to take up space.

To free up space taken by deleted files, use the Compact option in the File Manager Commands menu, or enter the Technician Interface **compact** *<volume>*: command. For example, enter **compact 2:** to compact the files in Volume 2. The file system copies all of the files to memory except for the deleted ones, erases the memory card, and copies the files back to the memory card.

When you copy any file on a memory card in a router running Version 7.80 or higher, the file system compares the size of the file with the amount of unused space on the memory card. If the file can fit in the unused space, the file system stores the file. If the file does not fit, the file system logs a message indicating the problem. However, if you save a file from the router's memory to the memory card, or transfer a file from an external device to the memory card using TFTP or FTP, and the memory card does not have space for the file, the file management system writes the file until it runs out of space, logs an "out of space" message, and aborts the save or transfer operation. If this occurs, delete the partial file and compact the files on the memory card.

To view the status of a memory card, display its directory. The directory display shows the amount of "available free space" or "free space," and the amount of "contiguous free space."

The "available free space" or "free space" is the total number of bytes of unused space and bytes of space used by files that are deleted.

In order for the memory card to accommodate a file, the file's size must be less than or equal to the "contiguous free space." The "contiguous free space" is the number of bytes of unused space.

If the file you want to store is less than the "available free space," but more than the "contiguous free space," compact the existing files first. When you finish compacting files on a memory card, the "contiguous free space" matches the "available free space."

Thus, if the directory display shows that the memory card has 1000 bytes of "available free space" and 1000 bytes of "contiguous free space," all of its free space is available for storing files. If you store a file that is 100 bytes, the number of bytes of "available free space" and "contiguous free space" each becomes 900 bytes. If you delete the file and display the directory, the display shows 1000 bytes of "available free space," but only 900 bytes of "contiguous free space." The 100-byte file remains on the memory card, even though you "deleted" it. Thus, only 900 bytes remain for storing additional files until you compact the existing files.

Memory or Buffer Problem

The router may have a memory or buffer problem if the log shows an "out of resources" or "memalloc" (memory allocation) error.

The router separates memory into these two types:

*   The router reserves global memory for all buffers.

    These buffers store all incoming and outgoing traffic.

*   The router reserves local memory for the router software image, the routing tables, and the forwarding tables.

    The router software image includes both the operating system and executable software modules.

Thus, the amount of local memory available determines the maximum number of entries in a forwarding or routing table. If the router has a shortage of local memory and an excess of global memory, you can use the configuration parameters in the Configuration Manager's Administration menu to increase available local memory. Refer to Table 3-3 to determine how much memory is available for the type of processor in your router.

Table 3-3.   Memory Configuration System Software Limitations

Processor Type	Memory Type				Increment By Which You Can Allocate Memory
	Minimum Local	Maximum Local	Minimum Global	Maximum Global	
FRE-II	4 Mb	30 Mb	2 Mb	16 Mb	2 Mb
ACE32 4 Mb	2624 Kb (2.56 Mb)	3 Mb	1 Mb	1472 Kb (1.43 Mb)	1 Kb
ACE32 8 Mb	2624 Kb (2.56 Mb)	7 Mb	1 Mb	4 Mb	1 Kb
ACE32 16 Mb	2624 Kb (2.56 Mb)	12 Mb	1 Mb	4 Mb	1 Kb
AFN 4 Mb	2624 Kb (2.56 Mb)	3 Mb	1 Mb	1472 Kb (1.43 Mb)	64 Kb
AFN 16 Mb	2624 Kb (2.56 Mb)	12 Mb	1 Mb	4 Mb	64 Kb
AN	1868 Kb (1.82 Mb)	16204 Kb (15.82 Mb)	180 Kb	14516 Kb (14.17 Mb)	1 Kb

To make sure the applications are loaded on the slot, enter the Technician Interface **loadmap** *<slot_no.>* command.

→ **Note:** *Do* not *insert a colon (:) after the slot no. in the* **loadmap** *command. (The colon applies only to media volumes, not to processor boards.)*

Example

```
$ loadmap 5
---------------------
Loadmap from SLOT 5:
---------------------
--> arp.exe          0x30af65c0  0008944
--> ftp.exe          0x30a4a8a0  0042676
--> tcp.exe          0x30a54f70  0057632
--> tftp.exe         0x30a630a0  0020680
--> snmp.exe         0x30a68180  0030360
--> tn.exe           0x30a73850  0038424
--> ip.exe           0x30a80ea0  0179700
--> ds2181.exe       0x30a10b80  0005640
--> hdlc.exe         0x30a13d60  0058272
--> e1.exe           0x30a7d4f0  0004032
```

The response shows the filename, starting offset (load address), and number of bytes of each dynamically loadable application running on the slot in question.

If a processor does not reside on a slot, the message `loadmap: no reply from slot(s) specified` appears.

Determine how your processor is currently using local and global memory as follows:

1. **To determine how the slot in question divides memory into global and local types, enter the following Technician Interface command:**

   get wfKernParamEntry.*._<slot_no.>_

   _<slot_no.>_ is the slot number of the processor module in the router. Use Slot 1 if you have an AN (Access Node).

2. **To display how the router is using memory, enter the following Technician Interface command:**

   get wfKernelEntry.*._<slot_no.>_

   The values that the Technician Interface displays include

   — How much memory is free

   — The starting PC (program counter [that is, address location in memory]) of the task.

   The Technician Interface displays each task as a PC code in the wfKernelEntry.wfKernelBufOwnerTask lines.

   — The number of buffers allocated for each task

Example

The most important lines in this example are in bold. This example shows only the most important lines in the display. It shows only a portion of what actually appears.

```
$ get wfKernelEntry.*.2
wfKernelEntry.wfKernelSlot.2 = 2
wfKernelEntry.wfKernelMemorySize.2 = 23752016
wfKernelEntry.wfKernelMemoryFree.2 = 21139840
. . .
wfKernelEntry.wfKernelBufOwnerTask1.2 = "315910F4"
. . .
wfKernelEntry.wfKernelBufOwnerTask2.2 = "31619B04"
. . .
```

```
wfKernelEntry.wfKernelBufOwnerTask3.2 = "31619B04"
wfKernelEntry.wfKernelMemOwnerTask1.2 = "3002923E"
.  .  .
wfKernelEntry.wfKernelMemOwnerTask3.2 = "30081CF6"
.  .  .
```

3. To determine which protocols are running, enter the following Technician Interface command:

loadmap *<slot_no.>*

➡ **Note:** *Issue the* **loadmap** *command on the same slot on which you entered the* **get wfKernelEntry.*.***<slot_no.>* *command. The order of the tasks change each time you boot a slot.*

Example

```
$ loadmap 2

--------------------
Loadmap from SLOT 2:
--------------------
--> arp.exe          0x31685720   0009784
--> vines.exe        0x315f47e0   0121448
--> ftp.exe          0x3164d6e0   0042868
--> tcp.exe          0x31657e70   0057776
--> tftp.exe         0x31666030   0020488
--> snmp.exe         0x3166b050   0030328
--> tn.exe           0x316726e0   0038424
--> ip.exe           0x31687d70   0182004
--> tms380.exe       0x3158ef80   0094428
--> hdlc.exe         0x31612260   0058496
--> dst.exe          0x315f3730   0004244
```

The loadmap display shows the protocols and other executable software modules running on the slot. Their associated starting PC codes are in hexadecimal format. The starting PC code of each wfKernelEntry attribute is a higher number than the PC code of its associated protocol.

The column on the right of the loadmap display shows the number of bytes assigned to the module. (If you convert the number of bytes to hexadecimal format and add it to the PC code to the left, the number equals the PC code of the next module in memory.)

Determining which protocol owns a task can help you determine which protocols are using the most memory. To do this, compare the PC code of the wfKernelEntry attribute with the starting PC codes in the loadmap display. Determine which PC code in the loadmap display is the next higher number, compared with the number in the wfKernelEntry display, and which is the next lower number. The protocol associated with the higher number owns the task.

Example

The following illustration shows another portion of the response to the **get wfKernelEntry.*.2** command.

```
$ get wfKernelEntry.*.2
. . .
wfKernelEntry.wfKernelMemOwnerTask6.2 = "315F7F08"
. . .
```

To make comparisons easier, the following illustration of the loadmap reorganizes the entries by PC code. You can determine that the PC code 315F7F08 is a higher number than the PC code associated with the *vines.exe* software module, and that it is lower than the next highest PC code in the display (*hdlc.exe*). Therefore, the task is a VINES task.

```
$ loadmap 2

---------------------
Loadmap from SLOT 2:
---------------------
--> tms380.exe      0x3158ef80   0094428
--> dst.exe         0x315f3730   0004244
--> vines.exe       0x315f47e0   0121448
--> hdlc.exe        0x31612260   0058496
--> ftp.exe         0x3164d6e0   0042868
--> tcp.exe         0x31657e70   0057776
--> tftp.exe        0x31666030   0020488
--> snmp.exe        0x3166b050   0030328
--> tn.exe          0x316726e0   0038424
--> arp.exe         0x31685720   0009784
--> ip.exe          0x31687d70   0182004
```

If a significant number of lack-of-resource errors are occurring, such as more than 50/min, report the problem to the Bay Networks Technical Response Center.

Bad Forward Checksum Errors

An event message beginning with "buf=" follows the bad forward reception buffer checksum error. Look at the text in bold in Figure 3-2.

```
mm/dd/yy 12:35:56 141.122.57.1 5 GAME W "bad fwd receive buffer checksum"

mm/dd/yy 12:35:56 141.122.57.1 5 GAME D "buf=0x801c1b30 - 0x00000000

0x801ce400 0xffc0001 1 0x007c04a4 0x306da810 - xsum=0xd7781ec8

0x801da86c - 0x00050004 0x0022d300 0x76c00000 0x76c00000

0x801da87c - 0x8b51704d 0x30682854 0x0f00bbbb 0x0004000A

0x801da88c - 0xf300001c 0x8638002b 0xb9f1 1240 0xc0000000

0x801da89c - 0x20009000 0xa4850452 0x0002030c 0x31303030

0x801da8ac - 0x39303238 0x41343835 0x30313032 0x50534552

0x801da8bc - 0x5645525f 0x41353039 0x00000000 0x00000000

0x80"
```

Figure 3-2.   Finding the Slot Number When the Message References a Backplane BOFL

Look at the number to the left of "GAME" on the first line. This is the number of the slot receiving the packet. In Figure 3-2, Slot 5 received the packet.

If multiple BOFL (breath of life) errors occur on the same sending or receiving slot, you may have a problem with the associated FRE processor.

The number 0x0f00bbbb indicates a backplane BOFL packet. A backplane BOFL packet is a BOFL packet sent from one slot to another to determine whether the destination slot is running.

Go to the appropriate section to determine which slot sent the BOFL packet:

- "Finding the Slot That Sent a Bad Backplane-BOFL-Packet" if the number 0x0f00bbbb is in the same location of your display as it is in Figure 3-2

- "Finding the Slot That Sent a Bad Packet That Was Not a BOFL Packet" if the number is *not* in the same location

Finding the Slot That Sent a Bad Backplane-BOFL-Packet

Determine which slot sent the BOFL packet that failed as follows:

1. **Find the number 0x0f00bbbb.**

2. **Find the number to right of the number 0x0f00bbbb.**

   In Figure 3-2, this number is 0x0004000A.

3. **Convert the last four digits of that number to decimal.**

   In the example, Slot 10 sent the bad backplane-BOFL-packet.

   ### *Example*

   0x000A = 10

4. **Call the Bay Networks Technical Response Center and describe the problem.**

   Depending on whether the slot sending or receiving the packet is always the same, it may be necessary to replace the processor.

Finding the Slot That Sent a Bad Packet That Was Not a BOFL Packet

Find the number of the slot that sent the packet by looking at the hexadecimal number that is in the same position as the number that is in bold in Figure .

```
mm/dd/yy 04:58:56 141.122.57.1 4 GAME W "bad fwd receive buffer checksum"
mm/dd/yy 04:58:56 141.122.57.1 4 GAME D "buf=0x801da800 - 0x00000000
0x801ce400 0xffc00011 0x007c04a4 0x306da810 - xsum=0xd7781ec8
0x801da86c - 0x00050004 0x0022d300 0x76c00000 0x76c00000
0x801da87c - 0x8b51704d 0xa0000012 0x221a090b 0x00000121
0x801da88c - 0xf300001c 0x8638002b 0xb9f11240 0xc0000000
0x801da89c - 0x20009000 0xa4850452 0x0002030c 0x31303030
0x801da8ac - 0x39303238 0x41343835 0x30313032 0x50534552
0x801da8bc - 0x5645525f 0x41353039 0x00000000 0x00000000
0x80"
```

Figure 3-3.   Finding the Slot Number When the Message Does Not Reference a Backplane BOFL

In the following example, the hexadecimal number in question is the 0xa000 portion of the number 0xa0000012. Convert the number to its binary equivalent.

Example

0xa000 = 1010 0000 0000 0000

In the binary representation of the number, a value of 0 means that the slot *did not* originate the message; a value of 1 means that the slot did originate the message. Ignore the leftmost digit. The digit to the right of the leftmost digit is the value for Slot 1, the next digit to the right is the value for Slot 2, and the next digit to the right is the value for Slot 3, etc. The right-most digit is meaningless because, at most, the router has only 14 slots. In this example, Slot 2 sent the message that failed.

Call the Bay Networks Technical Response Center and describe the situation. Depending on whether the slot sending or receiving the packet is always the same, it may be necessary to replace the FRE processor.

Fault Message

If a software entity experiences a fault and fails to recover, do the following:

1. **Disable and re-enable the port.**

   Watch the event log. Stop here if the software entity recovers.

2. **Reset the slot.**

   Watch the event log. Stop here if the software entity recovers.

3. **Press the Reset button on the front panel for no more than one second.**

   This initiates a warm-boot procedure, which will keep the log intact.

Caution: *Avoid using the **diags** command to boot a router after it has crashed. If you do so, or you remove and reinstall power, the diagnostics software overwrites the log. This prevents you from accessing it to determine the cause of the problem.*

   Watch the event log. Stop here if the software entity recovers.

4. **Save the log to a file and transfer it using FTP (File Transfer Protocol) or TFTP (Trivial File Transfer Protocol) to the Bay Networks host, or set the router up for modem access so that Bay Networks can dial in and look at it.**

   Go to Chapter 8 for instructions.

5. **Call the Bay Networks Technical Response Center to report the problem.**

Chapter 4
Troubleshooting a Physical Media Problem

This chapter describes how to solve physical media problems. It assumes you have already determined the scope of your problem, as described in Chapter 2.

This chapter includes the following sections:

- "Making Sure the Link Module Is Working"

- "Determining the Media-Specific State"

- "Troubleshooting the Cable Connection"

Making Sure the Link Module Is Working

Refer to the log to make sure that the link module and ports are enabled. If they are not, examine the log messages for the slot in question in order to determine whether they became disabled or never came up, and why.

Determining the Media-Specific State

Use the Statistics Manager Quick Get tool or the Technician Interface to check the media-specific state of the connector in question. Using the Quick Get tool, access wfLine➜wf<*MEDIA*>Table to retrieve the State attribute. Or, using the Technician Interface, enter the following command:

get <*object*>**.3.**<*slot_no.*>**.**<*connector_no.*>

<*object*> is one of the following: wfCSMACDEntry, wfSyncEntry, wfT1Entry, wfE1Entry, wfTokenRingEntry, wfFddiEntry, or wfHssiEntry.

The numeric identifier of the state attribute for these objects is 3.

For example, enter **get wfCSMACDEntry.3.1.4** to display the state of Ethernet in Slot 1, Connector 4.

You can use the wildcard character (*) to get the states of all connectors of a particular type on a slot, or all connectors of a particular type on the entire router. For example, enter **get wfCSMACDEntry.3.*** to display the state of all Ethernet connectors on the router.

Example

```
$ get wfCSMACDEntry.3.*
wfCSMACDEntry.wfCSMACDState.1.1 = 1
wfCSMACDEntry.wfCSMACDState.1.2 = 1
wfCSMACDEntry.wfCSMACDState.1.3 = 1
wfCSMACDEntry.wfCSMACDState.1.4 = 1
```

Refer to Table 4-1 for the meaning of the value of the attribute.

Table 4-1.   Values of Media State Attributes

Value	Meaning of State Attribute						
	CSMACD	Sync	T1	E1	Token Ring	FDDI	HSSI
1	up	up	up	up	up	up	up
2	down	down			down	down	LMI wait
3	initializing	initializing	initializing	initializing	initializing	initializing	BOFL wait

(continued)

Table 4-1.   Values of Media State Attributes *(continued)*

Value	CSMAC D	Sync	T1	E1	Token Ring	FDDI	HSSI
	Meaning of State Attribute						
4	not present	wait	not present	not present	not present	not present	CA wait
5		not present					initializing
6		DSR wait					not present
7		hold down					
8		remote loop					

Respond to State attribute values as follows:

1. **If the media-specific state of the interface in question is up, check the statistics associated with that layer.**

    If those statistics show that the media is OK, go to Chapter 6.

2. **If the state is not present, the dynamic loader did not load the driver (lower layer protocol) on the slot. Make sure the link or net module and port are up. Then make sure the driver runs on the slot in the configuration of the router.**

3. **If the state is down, check the log to determine the reason. Do the following:**

    a. **Save the log.**

    b. **Issue the clearlog command.**

    c. **Use the Configuration Manager to set the Enable parameter to Disable, or use the Technician Interface to set the Enable attribute to 2.**

    d. **Set the Enable parameter to Enable, or set the Enable attribute to 1.**

    e. **View the log.**

    f. **If the media-specific state is not up, test the cable and the transceiver.**

4. **If the cable and the transceiver are OK, use Packet Capture to test the reception and transmission of data as it passes through the cable. Refer to Appendix B for instructions.**

Troubleshooting the Cable Connection

Check the cable that carries the data as follows:

1. **If this problem occurred after connecting a new cable, make sure it is the proper cable for the application you are using. Refer to the *Cable Guide for Routers and BNX Platforms* for guidelines.**

2. **Make sure that both sides of the cable firmly connect to the proper interfaces.**

➡ **Note:** *Do not use the connector position in one link module to determine the position of another. Interface 1 of one type of link module may be on the left side and Interface 1 of another type may be on the right side. Verify the connection by looking at the connector number on the link module.*

3. **Check the LEDs on the rear panel of the router.**

    The green transceiver light goes on when the cable is secure.

    If you hot-swapped a link module or reset the slot, the associated red fail LED remains on until you run diagnostics on that slot. This condition does not necessarily indicate a problem. However, if you run diagnostics on a slot and the red fail LED remains on for more than a few minutes, call the Bay Networks Technical Response Center.

⊖ **Caution:** *Connect only cables that support hot swap to connectors that support hot swap. Also, connect only cables that do not support hot swap to connectors that do not. Otherwise, damage to the board may occur.*

4. **If the state of the connector is down, replace the cable.**

    Test whether the problem is the cable or the port by replacing it with a cable that you know is good.

5. **Perform local and remote loopback tests during network downtime, or on ports that are not in use.**

⊖ **Caution:** *Do not do loopback testing during production network time if the bridge is operating on the port.*

You can also loop back PPP lines. But if you configured them with a password, you must configure them in promiscuous mode first.

If you are accessing a DTE/DCE line with promiscuous mode off, the port will not increment the reception statistics.

If the connection is FDDI or ATM Rx and Tx,

a. **Make sure you cabled correctly the A and B ports.**

b. **Try looping Port A back to Port B to test for port failure.**

 If the Tx and Rx LEDs light, the ports and cable are OK.

c. **Check the event log to make sure that the router brings the ring up and marks the circuit as active.**

d. **If the loopback test fails, try a different fiber cable. Then try replacing the link module.**

Note: *Multimode fiber is orange, and single-mode fiber is yellow. The different fibers require different interface modules.*

Chapter 5
Troubleshooting a Data Link Connection Problem

This chapter describes how to solve data link layer problems. It assumes you have already determined the scope of your problem, as described in Chapter 2.

This chapter includes the following sections:

- "Troubleshooting an ATM Connection"
- "Troubleshooting an Ethernet Connection"
- "Troubleshooting an FDDI Connection"
- "Troubleshooting a Frame Relay Connection"
- "Troubleshooting an MCT1 Connection"
- "Troubleshooting a Synchronous Connection"
- "Troubleshooting a Token Ring Connection"
- "Troubleshooting Other Data Link Protocols"

Troubleshooting an ATM Connection

This section assumes that you have isolated a problem to an ATM connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot ATM as follows:

1. **Filter the log to display only messages from the ATM entity running on the slots experiencing the problem. The Technician Interface command is**

    log -fftwid -eATM -s<slot_no.>

    Example

    If you are filtering events from Slots 3 and 4, you enter

    log -fftwid -eATM -s3 -s4

➡️ **Note:** Configuring ATM Services *includes instructions on reading ATM log messages.*

2. **Use the Technician Interface to display the attributes associated with the wfAtmInterfaceConfEntry object.**

    The Quick Get path to this group is wfLine➤wfAtmInterfaceGroup➤ wfAtmCommonGroup➤wfAtmInterfaceConfTable.

    The instance associated with this object is the line no.

    These attributes show the configuration of the ATM port, including the aggregate cell rate and the maximum number of VCs on the port.

3. **Use the Technician Interface to display the attributes associated with the wfAtmVclConfEntry object.**

    The Quick Get path to this group is wfLine➤wfAtmInterfaceGroup➤ wfAtmCommonGroup➤wfAtmVclConfTable.

    The attributes show the VCL configuration, including the mode (direct, group, or hybrid), and the cell rates (burst, sustainable, or peak).

4. **Display the attributes associated with the wfAtmVclStatsEntry object.**

    The Quick Get path to this group is wfLine➤wfAtmInterfaceGroup➤ wfAtmCommonGroup➤wfAtmVclStatsTable.

The attributes include the number of cells received and transmitted, and the number of frames dropped.

5. **Display these attributes again after 1 minute and compare the values to determine which errors are currently occurring.**

   The wfAtmVclRcvCrcErrs attribute shows the number of errors due to line noise, which may be caused by defective fiber.

   The wfAtmVclRcvMaxLenExceedErrs attribute shows the number of packets coming from the ATM code and handed to the driver for transmission that exceeded the maximum MTU (maximum transfer unit) configured on the VCL. Check the configuration of the MTU and consider increasing the maximum MTU.

   The wfAtmVclRcvInvalidLenErrs attribute shows the number of SAR (segmentation and reassembly) frames containing an error in length after PDU (protocol data unit) re-assembly. It can indicate that the router is dropping frames. Check the dropped frame statistics. Check the path of the cells through the network to determine the location of the dropped cells.

6. **Use the Technician Interface to display the attributes associated with the wfAtmAlcCopDataPath object.**

   The Quick Get path to this group is wfLine� wfAtmInterfaceGroup� wfAtmLinkModule� wfAtmAlcCopDataPathTable.

   These attributes contain information on the ATM co-processor buffer utilization, the number of cells received and transmitted, and the number of dropped (clipped) frames.

   The count of each cell type received and transmitted is always 0; the other counts are for future use.

7. **Display these attributes again after 1 minute and compare the values to determine which errors are currently occurring.**

8. **Use the Technician Interface to display the attributes associated with the wfAtmAlcCopDataPath object.**

   The Quick Get path to this group is wfLine� wfAtmInterfaceGroup� wfAtmLinkModule� wfAtmAlcCopDataPathTable.

   These attributes contain the statistics showing how much data the link module is transmitting.

9. **Display these attributes again after 1 minute and compare the values to determine how much data the link module is currently transmitting.**

Refer to one of the following sections if it applies to your problem:

- "Dropped Frames"
- "ATM VC . . . Failed Message"
- "Upper-Layer Protocols Failing to Pass Packets"

Dropped Frames

Troubleshoot as follows:

1. **Enter the following command to display the value of the wfAtmAlcXmtPacketClips attribute:**

   get wfAtmAlcDrvEntry.29.*

2. **Enter this command again in 1 minute to determine whether the ATM port is dropping frames because of congestion on the outgoing queue.**

3. **Enter the following command to display the value of the wfAtmAlcCopRcvClipPackets attribute:**

   get wfAtmAlcCopDataPathEntry.11.*

4. **Enter this command again in 1 minute to determine whether the ATM port is dropping frames because of congestion on the incoming queue.**

5. **Determine which upper-layer protocols configured to run on the same port are receiving data.**

6. **Use Packet Capture and a network analyzer to determine which type of data is on the line.**

ATM VC . . . Failed Message

If the message "ATM VC mod failed" appears, the VC (virtual circuit) request to the driver failed. The message "VC ATM add failed" usually appears afterwards. Do the following.

1. **Check the VC definition in the configuration file and make sure that you defined the AAL (ATM adaptation layer) type as AAL 5.**

2. **Determine whether an oversubscription of the port cell rate occurred.**

3. **Make sure you used a VCI (Virtual Channel Identifier) number greater than 32.**

4. Match the error code in the message to the error code column in Table 5-1, and perform the associated instructions.

Table 5-1.   Error Codes in the "ATM VC mod failed" Log Message

Error Code	Meaning	Instructions
ATM_ERR_BAD_VC	The driver is already using the VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier).	Use a different channel.
ATM_ERR_NO_RESOURCE	The bandwidth is insufficient to satisfy the request.	Lower the cell rates.
ATM_ERR_NO_VC_AVAIL	The maximum no. of VCs are in already in use.	Increase the maximum no. of VCs.
ATM_ERR_COP_ERR	The coprocessor returned an error.	Document the error and call the Bay Networks Technical Response Center.

Upper-Layer Protocols Failing to Pass Packets

If the upper-layer protocols are failing to pass packets to ATM, do the following:

1. Find the message indicating that Data Path created a gate for the virtual circuit.

The message looks like this:

```
#  316: mm/dd/yy 14:57:42.417  DEBUG  SLOT  3  DP  Code:  23
Adding VC gate w/GH 0x627e to cct 3
```

The abbreviation "w/GH" stands for "with gate handle." A gate handle is the logical address of a process.

2. Check the subsequent log messages to make sure that the operating system did not subsequently kill this gate.

Troubleshooting an Ethernet Connection

This section assumes that you have isolated a problem to an Ethernet connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot as follows:

1. **Filter the log to display only messages from the CSMACD entity running on the slots experiencing the problem. The Technician Interface command is**

    log -fftwid -eCSMACD -s*<slot_no.>*

    Example

    If you are filtering events from Slots 3 and 4, you enter

    log -fftwid -eCSMACD -s3 -s4

2. **If only a single port on the slot is reporting errors, try switching out the transceiver/hub port the router is connected to, or the actual cable that connects the router to the transceiver cable or twisted-pair connection.**

    If the problem persists, verify the configuration of the Ethernet port. Then switch the problem connection to another Ethernet port. If the errors stop occurring, you may have a bad Ethernet port and should either replace the link module or call the Bay Networks Technical Response Center.

3. **Use the Technician Interface to look at the values of the following attributes in the wfCSMACDEntry object. Or, use the wfLine➤ wfCSMACDTable Quick Get path to access them.**

    *   wfCSMACDDelete

        This shows whether you configured CSMACD (1), or whether you did not (2).

    *   wfCSMACDEnable

        This shows whether CSMACD is enabled (1) or disabled (2) on the line.

    *   wfCSMACDState

        This shows whether CSMACD is up (1), down (2), initializing (3), or not present (4).

- wfCSMACDOctetsRxOk

  This shows the number of bytes received without error.

- wfCSMACDFramesRxOk

  This shows the number of frames received without error.

- wfCSMACDOctetsTxOk

  This shows the number of bytes transmitted without error.

- wfCSMACDFramesTxOk

  This shows the number of frames transmitted without error.

- wfCSMACDDeferredTx

  This shows the number of deferred transmissions. The Ethernet port detected a frame transmitting on the segment when it was preparing to transmit another frame. This is not an error, but an indication of a busy segment. If this statistic changes rapidly, determine why the segment is so busy.

- wfCSMACDLateCollnTx

  This shows the number of late collisions transmitted. A late collision transmission is a collision that takes place after the router transmits the first 64 bytes of a frame. The Ethernet Controller Chip (ILACC, Integrated Local Area Communications Controller) does not retransmit the frame. The length of the Ethernet cable exceeds the specified length. Replace it with a compliant cable.

  Late collisions may signify that the Ethernet LAN exceeds the length of the 802.3 IEEE (Institute of Electrical and Electronic Engineers) specifications.

- wfCSMACDExcessvCollnTx

  This shows the number of excessive collisions. The software declares an excessive collision when 16 successive attempts to transmit a frame fail because each attempt results in a collision. The router discards the frame and adds one to the error count.

  This is an indication of an overloaded segment with possible storms of data. Analyze this segment in order to determine what type of traffic is causing this problem.

- wfCSMACDBablErrorTx

  This shows the number of frames transmitted that were larger than 1518 octets. "BablErrorTx" stands for babbling transmitter errors. Despite declaring an error, the Ethernet controller chip transmits the packet in its entirety.

  Disable and enable the port and check the log for errors.

- wfCSMACDLcarTx

  This shows the number of loss of carrier errors, which is the number of times the port on the router lost the carrier connection during transmission to an external transceiver device. After carrier loss, the Ethernet controller chip continues to transmit the frame and the CSMACD entity logs an event. The controller chip does not retransmit the frame.

  This could indicate a bad transceiver cable, bad transceiver, or bad hub port.

- wfCSMACDFcsErrorRx

  This shows the number of frames Ethernet dropped upon receipt across this CSMACD line because the Ethernet controller chip detected a check sequence (checksum) error. The cause is usually physical.

  Make sure the cable connections are firm. Test the cables.

- wfCSMACDAlignErrorRx

  This shows the number of frames dropped upon receipt across this CSMACD line because the Ethernet controller chip detected a frame alignment error. An incoming frame contained a non-integer multiple of eight bits and a checksum error. If an incoming frame contains a non-integer multiple of eight bits, but does not have a checksum error, it does not increase this count. When this count is incrementing, the cause is usually physical.

  Make sure the cable connections are firm. Test the cables.

- wfCSMACDLackRescErrorRx

  This shows the number of receiver lack-of-resource errors. Indicates the number of times the router dropped packets it received because of a lack of buffers. The possibility that some lack-of-resource errors occur is likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the wfKernelEntry for the slot where the problem is occurring to determine whether free buffers are available, or to determine whether something on the network is preventing the router from updating its buffer lists. To do this, enter **get wfKernelEntry.*.<slot>**. For example: **get wfKernelEntry.*.2**. The router reports the number of available buffers in slot 2.

Check for protocol storms (for example, from IP RIP, IPX RIP and SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the wfCSMACDCfgRxQueueLength to 64, and see if that helps alleviate the problem.

•   wfCSMACDTooLongErrorTx

This shows the number of frames received that exceed 1518 octets. The router drops the frames because of a lack of space on the transmission queue (Tx). The possibility that some lack-of-resource errors occur is likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the wfKernelEntry for the slot where the problem is occurring to determine whether free buffers are available, or to determine whether something on the network is preventing the router from updating its buffer lists. To do this, enter **get wfKernelEntry.*.<slot>**. For example: **get wfKernelEntry.*.2**. The router reports the number of available buffers in slot 2.

Check for protocol storms (for example, from IP RIP, IPX RIP and SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the wfCSMACDCfgRxQueueLength to 64, and see if that helps alleviate the problem.

•   wfCSMACDMerr

This shows the number of Ethernet controller chip memory errors. The controller chip declares an error when it fails to access memory within 1512 clock ticks of asserting its data strobe signal. After declaring a memory error, the controller chip reinitializes. Go to "Memory or Buffer Problem" in Chapter 3.

- wfCSMACDCerr

  This shows the number of Ethernet controller chip collision detections. This is meaningful only if the attached transceiver or hub device implements an SQE (Signal Quality Error, also referred to as Ethernet Heartbeat) Test as defined in ANSI/IEEE 802.3. SQE specifies the periodic assertion of the transceiver's collision detection circuitry during down periods, and tests the integrity of the controller chip/transceiver connection.

  If the transceiver or hub device does not implement SQE, the value—0 or 1—is irrelevant.

  If the transceiver or hub device implements a SQE:

  – 0 indicates successful completion of the test.

  – 1 indicates that the SQE test failed. In this case, CSMACD logs an event noting SQE loss and verifies the integrity of the fuse. If the fuse is the problem, CSMACD logs another event and disables service to the line. If the fuse is OK, CSMACD retains service to the line.

- wfCSMACDTxClipFrames

  This shows the number of frames clipped in the driver's transmission routine due to transmission congestion. Check for the type of data that is transmitting. Determine whether a broadcast storm is disrupting the network, or whether the traffic is too heavy for the segment.

- wfCSMACDRxReplenMisses

  This shows the number of packet buffer misses while attempting to replenish driver reception ring. Another entity is using all of the available buffers. Go to "Memory or Buffer Problem" in Chapter 3.

- wfCSMACDUnAlignedFrames

  This shows the number of non-word-aligned frames received for transmission. A non-word-aligned frame means that the starting address of the data in memory is not an even number. Some protocol implementations in the router create non-word-aligned frames.

If the Ethernet controller is *not* a QENET, you can ignore this attribute. If the Ethernet controller is a QENET, check for underruns or corrupted frames. (This usually occurs only when you configure three or more ports on the QENET.) If underflow errors or corrupted frames occur, enable the attribute wfCSMACDAlignmentMode. This attribute determines whether the software aligns the frame on a word boundary before giving it to the QENET.

- wfCSMACDLateCollnRx

  This shows the number of late collisions received. A late collision reception is a collision that takes place after the router receives the first 64 bytes of a frame. The length of the Ethernet cable exceeds the specified length. Replace it with a compliant cable.

Troubleshooting an FDDI Connection

This section assumes that you have isolated a problem to an FDDI connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot an FDDI connection as follows:

1. **Filter the log to display only messages from the FDDI entity running on the slots experiencing the problem. The Technician Interface command is**

   log -fftwid -eFDDI -s<*slot_no.*>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eFDDI -s3 -s4

2. **Use the Technician Interface to look at the values of the following attributes in the wfFddiEntry object. The get command is next to the attribute name. Or, use the wfLine➜wfFddiTable Quick Get path to access them.**

   - wfFDDIOverrunRx (**get wfFddiEntry.16.***)

     This shows the number of frames received with internal overrun errors. The FSI (FDDI System Interface) chip set became overloaded and dropped packets.

- wfFDDIRingOverrunRx (**get wfFddiEntry.21.***)

  This shows the number of LLC (logical link control) reception ring overrun events. These errors are equivalent to "Lack of Resource" errors on a sync or Ethernet port. Each error indicates one lost packet. Troubleshoot a problem with reception ring overruns as follows:

  – Use the following command to verify how many buffers are currently free in the slot:

    get wfKernelEntry.*.*<slot>*

  – Go to "Memory or Buffer Problem" in Chapter 3 if you need an explanation of the memory issues.

  – Increase the size of the reception queue by setting the wfFddiEntry.43 attribute (wfFDDICfgRxQueueLength). The maximum setting is 255.

- wfFDDITxClipFrames (**get wfFddiEntry.40.***)

  This shows the number of frames clipped or dropped that the router could not add to the driver's transmission routine because of transmission congestion. Determine what type of data is overrunning the transmission port by using a network analyzer or the router's Packet Capture utility.

  Use the following command to verify how many buffers are currently free in the slot:

  get wfKernelEntry.*.*<slot>*

  Go to "Memory or Buffer Problem" in Chapter 3 for an explanation of the memory issues.

  Increase the size of the transmission queue by setting the wfFddiEntry.42 attribute (wfFDDICfgTxQueueLength). The maximum setting is 255.

3. **Enter the Technician Interface get wfFddiSmtEntry.9.* command. Or, use this Quick Get path to access it: wfLine➔wfFddiGroup➔ wfFddiSmtGroup➔wfFddiSmtTable➔wfFddiSmtCfState.**

   This shows the connection of the station to the ring. The codes are a follows:

- 1 = isolated
- 2 = wrap S
- 3 = wrap A

- 4 = wrap B

    This state indicates that the A and B ports connect to two different concentrators that connect to the same ring.

- 5 = wrap AB

- 6 = through

    This is the normal, non-wrap operating state for a dual-attached station.

- 7 = local A

- 8 = local B

- 9 = local AB

- 10 = local S

- 11 = cwrap A

    This state indicates that FDDI wrapped the A port of the FDDI link or net module because the B port is not receiving data.

    Make sure the B port cable is not disconnected, and the port is functional. One of the two fibers leading into the B port may be broken. Troubleshoot the cable.

- 12 = cwrap B

    This state indicates that FDDI wrapped the B port of the FDDI link or net module because the A port is not receiving data.

    Make sure the A port cable is not disconnected, and the port is functional. Troubleshoot the cable.

4. **Use the Technician Interface to look at the values of the following attributes in the wfFddiMacEntry object. The get command is next to the attribute name. Or, use this Quick Get path to access them: wfLine➔wfFddiGroup➔wfMacGroup➔wfFddiMacTable**

    - wfFddiMacUpstreamNbr (**get wfFddiMacEntry.4.***)

        This shows the MAC address of the upstream neighbor in the ring. Use it to determine whether the router wrapped the ring.

    - wfFddiMacDownstreamNbr (**get wfFddiMacEntry.5.***)

        This shows the MAC address of the downstream neighbor in the ring. Use it to determine whether the router wrapped the ring.

Troubleshooting a Frame Relay Connection

This section assumes that you have isolated a problem to a Frame Relay connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Filter the log to display only messages from the Frame Relay entity running on the slots experiencing the problem. The Technician Interface command is

log -fftwid -eFR -s<slot_no.>

Example

If you are filtering events from Slots 3 and 4, you enter

log -fftwid -eFR -s3 -s4

Refer to the symptoms identified in the sections that follow:

- "Log messages from Frame Relay Indicate Circuit Is Down"

- "Frame Relay Switch Keeps Marking the Circuit as Down"

- "Frame Relay Circuit Up, but Protocol Data Is Not Transmitting"

- "PVC Transmitting, but Not Receiving"

- "Frame Relay Configured with LMI Invokes an Xoff State"

Log messages from Frame Relay Indicate Circuit Is Down

Troubleshoot as follows:

1. **Check the Sync interface statistics to determine whether the Sync interface is receiving and sending traffic.**

2. **Make sure the status message timeout configurations of the switch and the router are the same.**

3. **Determine whether the virtual circuit and synchronous interface are receiving packets.**

4. **Make sure the circuit is enabled.**

Frame Relay Switch Keeps Marking the Circuit as Down

Troubleshoot as follows:

1. **Check the polling interval configuration on the switch and router.**

2. **Check the log for any events issued by Frame Relay to determine the status of the Frame Relay link.**

Frame Relay Circuit Up, but Protocol Data Is Not Transmitting

Troubleshoot as follows:

1. **Check the DLCI (data link control identifier) protocol configuration.**

2. **Check the routing tables for the correct routing information.**

3. **Check to see whether this problem is affecting all protocols or a single one.**

4. **Examine the FrVcError statistics to determine whether the router is dropping any packets.**

5. **Display the values of the VcCircuitEntry in order to determine whether the switch initiated flow control.**

6. **Display the wfFrVCircuitEntry values and check the number of FECNs (Forward Explicit Congestion Notifications) and BECNs (Backward Explicit Congestion Notifications).**

   The attribute names for FECNs and BECNs are wfFrCircuitReceivedFECNs and wfFrCircuitReceivedBECNs. The FECNs and BECNs indicate congestion on the network.

PVC Transmitting, but Not Receiving

If the log reveals that the PVC (permanent virtual circuit) is active, and the statistics reveal it is transmitting, but not receiving, do the following:

• Make sure that the Frame Relay switch at the remote side of the link supports the A-bit.

The switch sends the A-bit to the router to indicate it is up and active. If the switch does not support the A-bit, the router has no way of determining whether the remote side of the link is down, and thereby fails to disable the associated PVC.

• Determine whether the switch can loop back any data.

Frame Relay Configured with LMI Invokes an Xoff State

If a Frame Relay switch exceeds buffer thresholds and sends an R-bit, the router invokes an Xoff state. Xoff is equivalent to a disabled VC. The router brings down the DLCI/VC that received the R-bit, and the DLCI/VC goes away.

If the DLCI that received the R-bit is a Direct Mode DLCI, the router also disables all the upper-layer protocols associated with the DLCI.

If the DLCI is in Group Mode, the upper-layer protocols do not stop. In this case, the protocols may reroute.

You cannot configure the router to ignore an Xoff state. The software supports FECNs and BECNS in place of Xoff.

If IP is available, use the Ping trace option to determine which Frame Relay node is down.

Troubleshooting an MCT1 Connection

This section assumes that you have isolated a problem to an MCT1 (multichannel T1) connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

A includes instructions on reading MCT1 log messages.

Do the following if the connection is MCT1:

1. **Filter the log to display only messages from the MCT1 entity running on the slots experiencing the problem. The Technician Interface command is**

   log -fftwid -eMCT1 -s<slot_no.>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eMCT1 -s3 -s4

➡️ **Note:** *Appendix A includes instructions on reading MCT1 log messages.*

2. **Check the following MCT1 MIB entries by entering the following Technician Interface commands:**

   get wfDrivers.14.0

   Or, use the following Quick Get path to this attribute:
   wfSoftwareConfig➤wfDrivers➤wfMunichLoad.

   get wfLinkModules.17.0

   Or, use the following Quick Get path to this attribute:
   wfSoftwareConfig➤wfLinkModules➤wfMCT1E1Load.

3. **Make sure that the Line Type and Line Coding supplied by the T1 provider match the associated settings in the MCT1 configuration.**

4. **Make sure the DS0s (Directory Service 0) channels match at both the router and the central office.**

5. **Watch the LEDs in the back of the MCT1. If the Sync LED keeps flashing, the LBO (line build out; impedance or resistance on a line) is not in sync. Ask the T1 carrier if you should set it to long haul or short haul, and configure the LBO parameter accordingly.**

The Sync LED stays on when the framer is in sync with the carrier's clock.

6. **Make sure that you set the LBO appropriately.**

   For example, 0.0 dB is short haul (up to 133 ft).

7. **Use the MCT1 built-in BERT (Bit Error Rate Test) and Line loop-up, loop-down, and payload loopbacks for troubleshooting. (This feature is available only with Site Manager in dynamic mode.)**

   Note that only one port can be in BERT mode at a time.

   Payload loopbacks are available in extended super frame (ESF) line type mode only.

8. **Make sure that the clocking is set to Port1 Ext Loop or Port2 Ext Loop. These settings are equivalent to Sync External.**

   The internal clocking in the MCT1 link module is the same as the internal clocking of the T1 link module. The MCT1 Slave and Loop settings are equivalent to the T1 master clock in the T1 link module.

9. **Make sure the CRC16 (cyclic redundancy check) or CRC32 match the carrier's specifications.**

10. **Make sure that the Inter Frame Time Fill matches idles (0xFF) or flags (0x7E) with the remote end of the link.**

11. **Check the events from the entity DS1E1 (multichannel T1/E1 driver service) to view the MCT1 log entry events.**

    MCT1 uses the wfDs1E1 MIB entries. Therefore, the entity name associated with MCT1 is DS1E1, *not* MCT1.

    MCT1 uses the wfSyncEntry object; T1 uses the wfLogicalLineEntry object.

12. **Enter the Technician Interface loadmap <slot_no.> command and make sure that the software loaded the *munich.exe* and *mct1e1.exe* files. If it did not, use the Image Builder to add them to the router software image, and transfer the image to the memory card.**

Troubleshooting a Synchronous Connection

This section assumes that you have isolated a problem to a synchronous connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot a synchronous connection as follows:

1. **Filter the log to display only messages from the Sync entity running on the slots experiencing the problem. The Technician Interface command is**

   log -fftwid -eSYNC -s*<slot_no.>*

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eSYNC -s3 -s4

   If you see a message like the following, refer to "Troubleshooting the Internal Clock Settings (Lab Environments Only)" later in this chapter.

   ```
   Warning Sync Code: 40 "Connector COM2: clock speed does not
   match other ports."
   ```

2. **Use the Technician Interface to look at the values of the following attributes in the wfSyncEntry object. Display and record these statistics, wait 1 minute, and repeat. Compare the statistics shown each time to determine whether the media is currently experiencing problems. If the error statistics change, check the reception and transmission statistics of the other ports in the same slot.**

   The **get** command is next to the attribute name. Or, use this Quick Get path to access them: wfLine➜wfSyncTable.

   • wfSyncRuntsRx (**get wfSyncEntry.51.***)

   This shows the number of frames received that are smaller than minimum length. Usually indicates a clocking problem on the line.

   • wfSyncBadFramesRx (**get wfSyncEntry.49.***)

   Frames received that were unrecognizable. May indicate underflow errors or an out-of-phase clock on the remote side.

   • wfSyncLackRescRx (**get wfSyncEntry.42.***) and wfSyncLackRescRx: (**get wfSyncEntry.43.***)

This shows the number of times the router dropped frames it received because of a lack of buffers or a lack of space on the transmission queue. The possibility that some errors occur is likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the wfKernelEntry for the slot where the problem is occurring to determine whether free buffers are available. To do this, enter **get wfKernelEntry.*.<slot>**. For example: **get wfKernelEntry.*.2**. The router reports the number of available buffers in slot 2. If free buffers are available, something on the network is preventing the router from updating its buffer lists.

Check for protocol storms (for example, from IP RIP, IPX RIP and IPX SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the configured receive queue length (wfSyncCfgRxQueueLength) to 64, and see if that helps alleviate the problem.

- wfSyncUnderFlowTx (**get wfSyncEntry.44.***)

This shows the number of incomplete frames that the router transmitted because the device queue emptied.

This problem usually occurs when you out-clock the router's port. Certain link modules (such as the DSDE 5430) support only a 600-KB aggregate throughput; if the port is receiving a T1 clock signal, the link will be operational but underflow errors can occur.

3. **Refer to one of the following sections if it pertains to your problem:**

- "Checking the Address Format (Bay Networks Standard Only)"

- "Troubleshooting a Synchronous to X.21 Connection"

- "Reception Errors Incrementing or Reception Count Not Incrementing"

- "Troubleshooting the Internal Clock Settings (Lab Environments Only)"

Checking the Address Format (Bay Networks Standard Only)

If the router is running Version 7.0 or later of the Bay Networks Standard protocol, and you defined explicit addressing, make sure the addresses are in decimal format. (The addresses in a Series 5 router are in hexadecimal format.) If the address is greater than 9 and in the wrong format, the synchronous link fails to come up.

Troubleshooting a Synchronous to X.21 Connection

If you connect a Bay Networks router running Series 7 or Series 8 software to a device with an X.21 interface, do the following:

1. **Set the appropriate Com port jumpers on the Ethernet link module to the X.21 setting.**

   Refer to *Installing and Maintaining BN Routers* for instructions.

2. **Enter the following command:**

   get wfSyncEntry.76.*

3. **Make sure that you set the synchronous polling in the router's synchronous line driver configuration to 2 (disabled), which is the default setting.**

   If it is 1 (enabled) and the DSR (data set ready) lead drops, the software disables the synchronous driver. When you set the driver configuration to 2, the software disregards the DSR lead.

Reception Errors Incrementing or Reception Count Not Incrementing

Conduct a local loopback test of the local CSU (channel service unit) or DSU (digital service unit). During the loopback test, check the transmission and reception statistics. If the transmission and reception statistics increment equally without errors, conduct a loopback test of the remote CSU/DSU if at least one of the following is true:

• You configured the synchronous line as standard with explicit addressing.

- You configured the DTE/DCE (Data Terminal Equipment/Data Communication Equipment) with promiscuous mode turned on.

Caution: *Do not do loopback testing on a synchronous port during production network time if the bridge is operating on that port.*

The remote loopback test allows data to leave the router, cross the synchronous circuit to the remote CSU/DSU, and come back to the router.

If the transmission and reception statistics increment without errors, perform the local and remote loopback tests at the remote side.

If the local loopback test did not cause any error count to be incremented, but the remote loopback test did, request that the carrier test the line and remote CSU/DSU.

If the local loopback test causes the error counts to continue to increment, complete one of the following procedures in order to isolate the problem:

- Disconnect the cable from the port of the router reporting the errors and plug it into another port on the router that you know works correctly.

  If the synchronous errors persist, verify that you properly configured the newly tested port, test the cable, and test the local CSU/DSU.

  If the errors go away, compare the newly tested port's configuration to that of the original port. If the port configurations are the same, try swapping the link module that has the original port with a new link module.

- Or, connect the port of the router reporting the errors to another CSU/DSU and monitor the line statistics.

  If the errors persist, try another cable. If errors continue to persist, try swapping the link module with a new one.

Troubleshooting the Internal Clock Settings (Lab Environments Only)

If you are using crossover cables to connect to two back-to-back routers in a lab environment, make sure all interfaces on a given slot have consistent clock source and speed settings. Messages like the following appear if two interfaces on a slot have inconsistent clock settings:

```
Warning Sync Code: 40 "Connector COM2: clock speed does not match other
ports."
```

Note: *All internally clocked ports on a slot change to the last configured internal clock speed when you boot, save a dynamic configuration change, or enter the* **config** *command.*

Check the clock source and speed settings as follows:

1. **Enter the following command to display the clock source setting for each slot and connector in the router:**

   get wfSyncEntry.13.*

   The display shows the settings for all synchronous ports on all slots in the following format:

   ```
   wfSyncEntry.wfSyncClkSource.<slot_no.>.<connector_no.> = <setting>
   ```

   The setting is 1 for clocking within the router or 2 for clocking from an external source.

2. **If any of the clock source settings are 1 (for internal clocking), enter the following command to check the clock speed:**

   get wfSyncEntry.14.*

   The console displays the transmission and reception clock speed for each slot and connector on the router. All ports configured for internal clocking within a slot use the clock speed of the port most recently configured for internal clocking. The clock speed is valid only for the slots that are set for internal clocking.

   The clock speeds you can set are 1200 (1200b), 2401 (2400b), 4807 (4800b), 7204 (7200b), 9615 (9600b), 19230 (19200b), 32051 (32000b), 38461 (38400b), 56818 (56k), 64102 (64k), 125000 (125k), 227272 (230k), 416666 (420k), 625000 (625k), 833333 (833k), 1250000 (1mb), 2500000 (2mb), and 5000000 (5mb).

Troubleshooting a Token Ring Connection

This section assumes that you have isolated a problem to a Token Ring connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot Token Ring as follows:

1. **Filter the log to display only messages from the Token Ring entity running on the slots experiencing the problem. The Technician Interface command is**

   log -fftwid -eTOKEN -s<slot_no.>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eTOKEN -s3 -s4

   If Token Ring Debug Event 36 ("Connector MAU<SlotConnector> Ring Status Change<4_digit_hex_code>)" appears, convert the 4-digit number from hexadecimal to binary. Assign the position numbers 0 through 10 to the first 11 digits from left to right. Look for the position number of the "1" bit in the following list:

   - 0 indicates signal loss.

   - 1 indicates a hardware error.

   - 2 indicates a software error.

   - 3 indicates a transmitter beacon.

   - 4 indicates a lobe wire fault.

   - 5 indicates an automatic removal error.

   - 6 is reserved for future use.

   - 7 indicates a remove received.

   - 8 indicates a counter overflow.

   - 9 indicates a single station.

   - 10 indicates a ring recovery.

2. **If you are using the Technician Interface, enter the following command to list the instances of the wfTokenRingEntry object:**

   list instances wfTokenRingEntry

3. **If you are using the Technician Interface, enter the following command to display the values of the wfTokenRingEntry object for the instance in question:**

   get wfTokenRingEntry.*.*<instance>*

   Or, use the wfLine➜wfTokenRingTable Quick Get path to access them.

4. **Look at the values of the following attributes:**

   • wfTokenRingMadrSelect

   This shows the source of the MAC address: boxwide (1), PROM (2), or configuration (3).

   • wfTokenRingSpeed

   This shows whether the speed is 4 Mbps (4194304) or 16 Mpbs (16777216).

   • wfTokenRingEarlyTokenRelease

   This shows whether Early Token Release is enabled (1) or disabled (2). It is valid only when the ring speed is 16 Mbps.

Troubleshooting Other Data Link Protocols

This section assumes that you have isolated a problem to a data link connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot a data link protocol not mentioned previously in this chapter as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the media in question.**

    The Technician Interface command is

    log -fftwid -e<ENTITY> **-s**<slot_no.>

    Example

    If you are filtering events from the HSSI entity running in Slots 3 and 4, you enter

    log -fftwid -eHSSI -s3 -s4

    When specifying the <ENTITY>, use uppercase letters. Refer to *Event Messages for Routers and BNX Platforms* for a list of the entities.

2. **Check the state of the media.**

3. **Check the values of the following statistics twice and compare them to determine whether the media is currently receiving and transmitting frames, and generating errors:**

    *   The reception and transmission statistics

        If the reception or transmission statistics do not change, do the following:

        — Check the reception and transmission statistics of the other ports in the same slot.

        — Try disabling and enabling the port, and watch the log messages to determine why the connection will not come up.

    *   The error statistics

4. **Look at the forwarding tables of each router in the path to determine**

    *   Whether entries exist

    *   Whether the next-hop addresses are in the right direction

5. **Verify the configuration parameters.**

6. **Use Packet Capture and a network analyzer to check the segments involved in the problem.**

Chapter 6
Troubleshooting a Network Connection Problem

This chapter describes how to solve network layer problems. It assumes you have already determined the scope of your problem, as described in Chapter 2.

This chapter includes the following sections:

- "Troubleshooting AppleTalk"
- "Troubleshooting DLSw"
- "Troubleshooting IP"
- "Troubleshooting IPX"
- "Troubleshooting OSI"
- "Troubleshooting Switched Services"
- "Troubleshooting Other Networking Protocols"

Troubleshooting AppleTalk

This section assumes that you have isolated a problem to AppleTalk. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot AppleTalk problems as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for AppleTalk.**

   The Technician Interface command is

   log -fftwid -eAT -s<i><slot_no.></i>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eAT -s3 -s4

2. **Enter the following command to check the base records:**

   get wfAppleBase.*.0

   The most important attributes are

   • The State attribute shows whether AppleTalk is up (1), down (2), initializing (3), or not present (4). You cannot change this setting.

   • The Disable attribute reveals whether AppleTalk is enabled (1) or disabled (2).

3. **Check the values of the following statistics twice and compare them to determine whether AppleTalk is currently receiving and transmitting packets, and generating errors:**

   • The reception and transmission statistics

     If the reception or transmission statistics do not change, do the following:

     — Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.

     — Try disabling and enabling AppleTalk, and watch the log messages to determine why the connection will not come up.

   • The error statistics

4. **Make sure that the next hop and network you are trying to reach are in the routing table entries.**

5. Verify the configuration parameters.

6. Use Packet Capture and a network analyzer to check the segments involved in the problem.

The following sections describe how to respond to certain event messages from AppleTalk:

• "Local Net Range Conflict Event Message"

• "Zone . . . Conflict Event Message"

• "Static Configuration Conflict Event Message"

Local Net Range Conflict Event Message

Configure the router's interface to match the network range configured on the seed router.

The configured network range failed to match that of another seed router's defined network range. The router sent a request for network information and received a response that contained a network range that was inconsistent with that configured for the interface.

Zone . . . Conflict Event Message

If the message `Zone Name Conflict`, `Number of Zones on Extended Net Conflict`, or `Default Zone-Seed Conflict` appears in the event log, configure the router's interface to match the zones configured on the seed router.

The configured network range failed to match the defined zones of another seed router. The router sent a ZIP (Zone Information Protocol) request and received a response that contained zone information that was inconsistent with that configured for the interface.

The message `Number of Zones on Extended Net Conflict` appears if a zone other than the default zone fails to match that of the seed router, or if the default zone name is in the zone list. The default zone should not be in the zone list.

The message `Default Zone - Seed Conflict` appears if the default zone fails to match that of the seed router.

Static Configuration Conflict Event Message

The node number associated with the interface is already in use by another node on the same segment.

Set the node number of the interface to 0 so that it will configure dynamically, or define a unique node ID.

Troubleshooting DLSw

This section assumes that you have isolated a problem to DLSw. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

You can turn on extended DLSw (Data Link Switch) log messages by setting the Max Sessions attribute under wfDls to 1111. We recommend that you turn off extended DLSw messages when you finish examining the log to test or troubleshoot a DLSw connection.

Troubleshoot DLSw as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for DLSw.**

   The Technician Interface command is

   log -fftwid -eDLS -s<i><slot_no.></i>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eDLS -s3 -s4

2. **Make sure that the DLSw MTU size matches the synchronous line MTU size.**

   Unnecessary packet fragmentation can occur when these settings do not match.

3. **Use the Technician Interface or the Statistics Manager to inspect the global source-route bridge settings, such as the internal LAN ID, the group LAN ID, and the bridge ID. If you are using the Technician Interface, enter the following command:**

   get wfBrSr.*.0

4. **Use the Technician Interface or the Statistics Manager to inspect the global DLSw settings, such as the configured TCP window size and the total number of established DLSw sessions. If you are using the Technician Interface, enter the following command:**

   get wfDls.*.0

   Make sure that the virtual ring ID for the IP cloud is unique and is consistent among all sites.

5. **Use the Technician Interface or the Statistics Manager to inspect the state of all of the DLSw interfaces currently configured, and the value of the instance field. If you are using the Technician Interface, enter the following command:**

   get wfDlsInterfaceEntry.3.*

6. **Use the Technician Interface or the Statistics Manager to inspect the state of all of the TCP connections. If you are using the Technician Interface, enter the following command:**

   get wfTcpConnEntry.2.*

   Make sure all active TCP sessions are in an "established" state (represented by the value "5").

   If the sessions are in an established state, the local and remote DLSw TCP slot/peer configuration is probably correct.

   If the sessions are not in an established state, do the following:

   a. **Make sure all slots configured to run DLSw have a slot IP address assigned.**

   b. **Make sure that the slot IP address corresponds to the DLSw Peers setting at the remote site.**

7. **Use the Technician Interface or the Statistics Manager to inspect the reception messages and connection state changes.**

Troubleshooting IP

This section assumes that you have isolated a problem to IP. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot IP as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for IP running on the slots in question.**

   The Technician Interface command is

   log -fftwid -eIP -s<slot_no.>

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eIP -s3 -s4

2. **Enter the following command to check the base records:**

   get wfIpBase.*.0

   The most important attributes are as follows:

   - The State attribute shows whether IP is up (1), down (2), initializing (3), or not present (4).

     You cannot change this setting.

   - The Create attribute reveals whether IP is created (1) or deleted (not 1).

   - The Enable attribute reveals whether IP is enabled (1) or disabled (2).

   - The Forwarding attribute reveals whether IP forwards (1) or does not forward (2) datagrams received by it, but not addressed to it.

   Example

   ```
   $ get wfIpBase.*.0
   wfIpBase.wfIpBaseCreate.0 = 1
   wfIpBase.wfIpBaseEnable.0 = 1
   wfIpBase.wfIpBaseState.0 = 1
   wfIpBase.wfIpBaseForwarding.0 = 1
   wfIpBase.wfIpBaseDefaultTTL.0 = 30
   wfIpBase.wfIpBaseRipDiameter.0 = 15
   wfIpBase.wfIpBaseRouteCache.0 = 60
   wfIpBase.wfIpBaseMibTables.0 = 2
   wfIpBase.wfIpBaseNetworks.0 = 250
   ```

```
wfIpBase.wfIpBaseZeroSubnetEnable.0 = 2
wfIpBase.wfIpBaseEstimatedNetworks.0 = 0
wfIpBase.wfIpBaseHosts.0 = 81
wfIpBase.wfIpBaseEstimatedHosts.0 = 0
wfIpBase.wfIpBaseDefaultOverSubnetEnable.0 = 2
wfIpBase.wfIpBaseMaxPolicyRules.0 = 32
```

3. **Check the values of the following statistics twice in the wfIpInterfaceEntry object. Compare them to determine whether IP is currently receiving and transmitting packets, and generating errors:**

   • The reception and transmission statistics

     If the reception or transmission statistics do not change, do the following:

     — Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.

     — Try disabling and enabling IP, and watch the log messages to determine why the connection will not come up.

Caution: *Do not do this if it could be disruptive to the network.*

   • The error statistics

4. **Make sure that the next hop and network you are trying to reach are in the routing table entries.**

5. **Verify the configuration parameters.**

6. **Use Packet Capture and a network analyzer to check the segments involved in the problem.**

Refer to one of the following sections if it pertains to your problem:

• "Troubleshooting Telnet, FTP, and TFTP"

• "Ping Does Not Work"

• "Troubleshooting Routing Information Protocol (RIP)"

• "Troubleshooting Open Shortest Path First (OSPF)"

Troubleshooting Telnet, FTP, and TFTP

The message Unknown Network or Network Unreachable indicates that the device does not have a path to the requested network.

If the sender and the target are on the same LAN, verify that the network IP address and subnet mask are the same for both interfaces.

If this message appears on a UNIX workstation, issue the **netstat -r** command at the workstation. The workstation displays the contents of the routing table, along with any default routes present. Check the port's subnet mask, which determines whether networks are local or remote. If the workstation is in routed mode, check the daemon's configuration.

Troubleshoot Telnet, FTP, or TFTP as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the application.**

    The Technician Interface command is

    log -fftwid -e<TELNET | FTP | TFTP>

    Example

    If you are filtering events from Telnet, you enter

    log -fftwid -eTELNET

2. **Enter the following command to check the base records:**

    get <wfTelnet | wfFtp | wfTftp>**.*.0**

    Example

    get wfTelnet.*.0

    The Delete attribute appears only in the Telnet and FTP base records. It reveals whether the protocol is created (1) or deleted (2).

    The Disable attribute reveals whether the protocol is enabled (1) or disabled (2).

3. **Ping your interface address.**

4. **Ping the next-hop address listed in the routing table for the network on which the remote host resides.**

5. **Make sure that the ICMP echo outs statistic is increasing for the IP interface.**

6. **Use the `ping -p` command to trace the path the ping is taking, look for loops, and determine whether the packet's TTL (time to live) field times out.**

   The message `Unreachable` indicates that IP does not have a route to the network in the routing table and cannot issue a ping request.

   The message `Does not respond` indicates that the router did not receive a response to the ping request.

7. **Check the cabling on the local and remote devices.**

8. **Make sure the application is running on the local and remote devices.**

9. **Make sure the circuit is enabled and up.**

10. **Make sure the interface is enabled and up.**

11. **Make sure the next hop address in the routing table**

   a. **Is its own interface address for any directly connected network**

   b. **Is the address of another router's interface on a directly connected network for any non-directly connected network**

Ping Does Not Work

Complete the instructions in the sections that apply:

- "Router Cannot Ping Another Local Device"

- "Router Cannot Ping Endstation, but Can Ping Other Endstations on the Same Segment"

- "Endstation Cannot Ping the Remote Interface on the Router"

- "Endstation Can Ping Devices on the Same Segment, but Cannot Ping the Router"

- "Endstation Can Ping Local and Remote Interfaces on the Router, but Cannot Ping a Remote Station"

→ **Note:** *The source address used in any ping (ICMP echo request) originating from the router is always the IP address of the router's outgoing port.*

Router Cannot Ping Another Local Device

When the router cannot ping another device on the network, it does not necessarily mean that the network or router is down.

If the device you are trying to ping never responded successfully to a ping request before because it is a new endstation, a new segment, or a new router, make sure that you configured it properly.

If the ping was successful at one time, and is no longer successful, try to isolate the problem to any recent changes in the network. If you do not know of any recent changes, or if you verified that they are OK, do the following:

1.   **Try to make the endstation ping itself.**

     If the endstation cannot ping itself, refer to the manuals on the TCP/IP stack and LAN card for that system and inspect the installation and configuration.

     An endstation must be able to ping itself in order to receive a ping response from the network. However, the self-ping operation is internal, and has nothing to do with the network or the router. Therefore, an incorrectly configured endstation may be able to ping itself just as easily as a correctly configured endstation.

2.   **Try to make the router ping its own interface.**

     If the router can ping its own interface, it enabled the interface and the protocols configured on the port. However, like an endstation, a misconfigured router may be able to ping itself.

     If the router cannot ping its own interface, check the log and verify the physical status of the interface.

3.   **Try to make the endstation ping other interfaces on the same router.**

4.   **Try to make the endstation ping other devices on the same segment.**

5.   **Enter the Technician Interface loadmap** *<slot_no.>* **command for each slot and verify that IP and ARP are running on all slots.**

6.   **Verify that the ARP cache only has entries for hosts on the local network.**

     Refer to the MIB object wfIpNetToMediaEntry to locate the ARP cache.

Router Cannot Ping Endstation, but Can Ping Other Endstations on the Same Segment

If the router can ping other endstations successfully, but not the endstation in question, and the endstation in question cannot ping other nodes on the network, do the following:

1. **Verify that the configuration of the endstation is correct.**

2. **Verify that the router's ARP cache contains the endstation's MAC address.**

   Refer to the MIB object wfIpNetToMediaEntry to locate the ARP cache.

   If the MAC address is incorrect, go to the endstation and try to ping the router. The router should update its ARP cache with the correct MAC address. The router's ARP cache entries do not age out unless you enable the HOST/ARP cache.

3. **Look for an entry with alternating MAC addresses.**

   If an entry is alternating between one MAC address and another, two devices on the network have duplicate IP addresses. Change the IP address of one of the devices.

Endstation Cannot Ping the Remote Interface on the Router

Refer to one of the following sections:

- "Network Unreachable Message"

- "Host Did Not Respond Message"

Network Unreachable Message

Verify that the endstation's configuration includes a default gateway.

If an endstation tries to send data to another IP address, it uses its own subnet mask to determine whether the destination is on the same segment (that is, the same network and subnet), or a remote segment (that is, a different network and/or subnet).

If the destination address is on a remote segment, and the endstation's configuration includes a default gateway, it tries to route the packet via the gateway. If the endstation's configuration does not include a default gateway, it displays a `network unreachable` message.

Host Did Not Respond Message

If the endstation or router displays this message, do the following:

1. **Make sure that the endstation configuration includes a default gateway definition or listens to a routing protocol.**

2. **Verify the network addresses of the source and destination devices.**

3. **If the node that did not respond is on a remote segment, make sure that each router is correctly resolving the ARP address of the next device in the path.**

4. **If the node that did not respond is on the local segment, use the wfIpInterfaceEntry MIB object to verify the address configuration and interface ICMP counters.**

Endstation Can Ping Devices on the Same Segment, but Cannot Ping the Router

If the endstation can ping other devices on the same segment, but cannot ping the local interface of the router, do the following:

1. **Compare the endstation's interface number, network number, and subnet mask to those of the router's interface. The network and subnet numbers must be the same, except that the endstation's subnet mask does not have to include as many octets as the router's (Figure 6-1).**

Network 129.122.32.0
Interface 129.122.32.1
Subnet mask 255.255.255.0

Router

Host

Network 129.122.0.0
Interface 129.122.32.66
Subnet mask 255.255.0.0
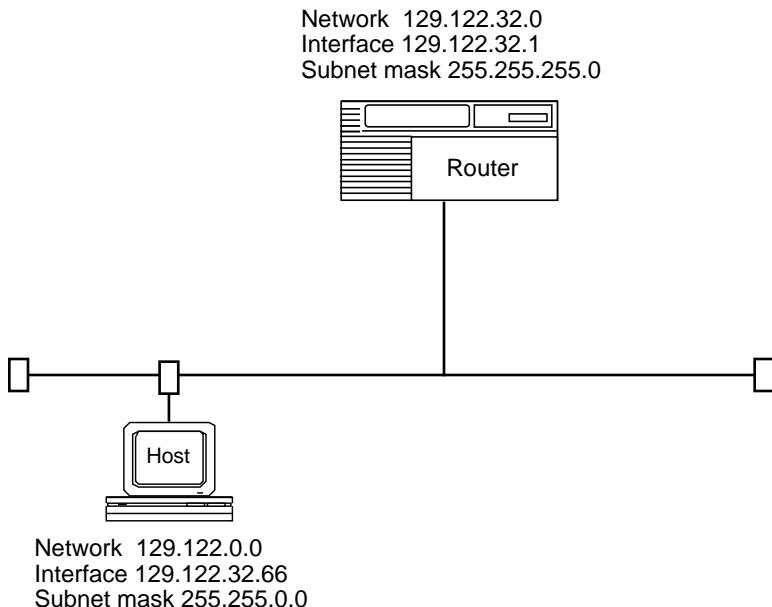
Figure 6-1.   Comparing the Endstation and Router Configurations

The subnet mask allows the router to determine which traffic to route to each segment. In Figure 6-1, the router's subnet mask must include the third octet if other subnets in the 129.122 network connect to the router. Usually in such configurations, you configure Proxy ARP (Address Resolution Protocol) to run on the router's interface because the endstation does not know that it has to go through the router to get to other subnets of the 129.122.0.0 network.

2. **Disable IP on the router's interface, and try to ping the IP address of the router again.**

If the ping succeeds, a device with a duplicate IP address is on the segment.

3. **Enable IP on the router's interface and try to ping other stations on the segment that is reporting problems.**

If the attempts to ping fail, verify that you configured the router with the correct IP network, interface, and subnet addresses.

Endstation Can Ping Local and Remote Interfaces on the Router, but Cannot Ping a Remote Station

Do the following:

1. **Ping the device on each link in the path between the source and destination to determine the location of the problem.**

➡ **Note:** *Use the Site Manager or Technician Interface "path" option when pinging the remote station. This option provides the same functionality as* **traceroute** *does on a UNIX workstation.*

2. **Make sure that the "next hop" for each network points to the correct interface.**

3. **Ping from the remote station to the local station.**

   This verifies that each router in the path not only has a route to the remote segment but also has a path back to the originator of the ping request.

Troubleshooting Routing Information Protocol (RIP)

If the router cannot reach a network or host, determine whether the entry is in the routing table.

If the entry is in the routing table, determine whether the next hop and metric are correct.

If the entry is not in the routing table, do the following:

1. **Determine whether the router enabled RIP.**

2. **Set RIP Listen on the RIP interface.**

3. **Determine whether a RIP station on an attached network is sending RIP packets.**

4. **Use Packet Capture or a network analyzer to capture the RIP packets and verify the accuracy of the advertisements from other RIP stations.**

Troubleshooting Open Shortest Path First (OSPF)

Do the following to troubleshoot an OSPF routing problem:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for OSPF running on the slots in question.**

    The Technician Interface command is

    log -fftwid -eOSPF -s*<slot_no.>*

➡ **Note:** *In Version 8.01 and higher, you can restrict the amount of OSPF information that appears in a log. Remove these filters when trying to troubleshoot a problem.*

    ### *Example*

    If you are filtering events from Slots 3 and 4, you enter

    log -fftwid -eOSPF -s3 -s4

2. **Enter the following command to check the base records:**

    get wfOspfBase.*.0

    The most important attributes are as follows:

    *   The State attribute shows whether OSPF is up (1), down (2), initializing (3), or not present (4).

        You cannot change this setting.

    *   The Create attribute reveals whether OSPF is created (1) or deleted (not 1).

    *   The Enable attribute reveals whether OSPF is enabled (1) or disabled (2).

3. **Check the OSPF neighbor states to determine the exchange state with other OSPF routers on the network.**

    Neighbor states should be either two-way or full; the other states (init, exchange start, or loading) are interim or transition states. Investigate any routers or links that do not recover from these states.

4. **Look at the link state data base (LSDB) of the router.**

    This is the information from which the router builds its routing table.

5. **Enter the following command to display the IP forwarding table:**

   get wfIpBaseRtEntry.7.*

   The Technician Interface displays the table in the following format:

   ```
   wfIpBaseRtEntry.wfIpBaseRouteNextHop.<network> = <next_hop>
   ```

   Identify the incorrect routes. If you take a snapshot of your network periodically, as described in Chapter 1, comparing the data can help you to identify the incorrect routes.

   Use the Packet Capture utility or a network analyzer to trace routes through the network to see what, if any, nodes are forwarding incorrect routing information in the form of RIP or Link State packets.

6. **Determine whether the link is operational and the communication is bi-directional. You can do this by getting the MIB object wfOspfIfEntry. The display shows the state of OSPF on the interface, the identity of the DR and BDR on the segment, how many hello packets the interface received and transmitted, and how many link state updates it received, and received and transmitted.**

Troubleshooting IPX

This section assumes that you have isolated a problem to IPX. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

This section assumes that you have loaded the scripts. Refer to *Using Technician Interface Scripts* for instructions.

Troubleshoot IPX as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for IPX running on the slots in question.**

   The Technician Interface command is

   log -fftwid -eIPX -s*<slot_no.>*

   Example

   If you are filtering events from Slots 3 and 4, you enter

   log -fftwid -eIPX -s3 -s4

2. **Make sure that the IPX routing software is up.**

To do this, use the Statistics Manager Quick Get Facility to display the value of wfApplication➜wfIpxGroup➜wfIpxBaseState, or use the Technician Interface to load the scripts and enter the following Technician Interface script command:

show ipx base

Example

```
$show ipx base
IPX Base Record Configuration Information
-----------------------------------------
Protocol   State    Router Name
--------   -----    -----------
IPX        Up       1
Primary NN                 Router Name
-----------  -------------------------------------------------
None          None

Route Method Mult Host Mode  Maximum Path
------------ --------------- ------------
Tick Based   Enabled                    1

Log Filter Setting      PreConfigured Net Table Size
----------------------------  -----------------------------
Filter Trace                                            0
```

3. **Make sure that each configured network is in the up state, and that the network address, host address, and encapsulation method are correct for each circuit.**

To do this, use the Statistics Manager to view the IPX Main Information Table screen, or enter the following Technician Interface script command:

show ipx circuit

Example

```
$show ipx circuit

IPX Circuit Configuration Information (ALL)
-------------------------------------------

Circuit   State    Net Address     Host Address     Encaps Method
 --------  -------- ------------   ----------------  -------------
O22       Up       0x2E000011      0x0000A20E08D4    LSAP
E44       Up       0x2E008000      0x0000A2030079    Ethernet
E32       Up       0x2E009000      0x0000A2035A5E    LSAP
E33       Up       0x2E010000      0x0000A2035A5F    LSAP
E42       Up       0x2E036000      0x0000A2030077    Novell/802.3
O21       Up       0x2E060010      0x0000A20E08D3    LSAP
O23       Up       0x2E060100      0x0000A20E08D5    LSAP

7 Circuits in table.
```

Note: *If an interface running IPX and Bridge receives a packet with an IPX encapsulation type that is different from that configured on the interface, the Bridge sends it to other interfaces running Bridge. IPX reads only the IPX packet encapsulation types that you configure it to read. Therefore, you must be careful when configuring the packet encapsulation types in an IPX network.*

4. **If you configured the router to run RIP, make sure that IPX RIP is up on the circuits in question.**

   To do this, use the Statistics Manager to view the IPX RIP Interface Table screen, or enter the following Technician Interface script command:

   show ipx rip

   The RIP Interface Table shows whether you configured the RIP interfaces with RIP Supply, RIP Listen, or Standard (both RIP Supply and RIP Listen).

Example

```
IPX RIP Interface Record Configuration Information (All)
-------------------------------------------------------

RIP
Interface     State     Mode
-----------   -------   -------
0x2E000011    Up        Standard
0x2E008000    Up        Standard
0x2E009000    Up        Standard
0x2E010000    Up        Standard
0x2E036000    Up        Standard
0x2E060010    Up        Standard
0x2E060100    Up        Standard
```

5. **Make sure the networks you are trying to reach are in the IPX routing table.**

   To do this, use the Statistics Manager to view the IPX Base Route Table screen, or enter the following Technician Interface script command:

   show ipx routes

   ### Example

   ```
   $show ipx routes

   IPX Routing Table Information
   ----------------------------
   Destination   NextHop Net   NextHop Host     Method Age Ticks Hops
   -----------   -----------   --------------   ------ --- ----- ---
   0x00000002    0x2E060100    0x0000454B2F59   RIP    20   21    12
   0x00000003    0x2E060100    0x0000454B2F59   RIP    20   23    13
   0x00000022    0x2E060010    0x000045B0F556   RIP    10   15     5
   0x00000023    0x2E060010    0x000045B0F556   RIP    10   16     6
   0x00000024    0x2E060100    0x0000454B2F59   RIP    20   15     5
   0x00000025    0x2E060100    0x0000454B2F59   RIP    20   15     5
   0x00000042    0x2E060100    0x0000454B2F59   RIP    30   18     8
   ```

   Alternatively, you can display a route to a specific destination by entering the following Technician Interface script command:

   show ipx route find *<destination_address>*

Example

```
$show ipx route find 0x00000986
IPX Routing Table Information
----------------------------
Destination  NextHop Net NextHop Host   Method Age Ticks Hops
-----------  ----------- ------------- ------ --- ----- ---
0x00000986   0x2E000011  0x0000C9108A7A RIP 20  2     1
```

6. **Examine the entries in the routing table to make sure that the path to the destination in question is appropriate.**

7. **Make sure that the server you are trying to reach is in the IPX SAP table.**

    To do this, use the Statistics Manager to view the IPX Base SAP Table screen, or enter the following Technician Interface script command:

    show ipx services

Example

```
$show ipx services
IPX Service Table Information
----------------------------
                  Server                    Service  Age  Hops
                                            Type
----------------------------------------- -------- ----- --
QDS                                         0x0004   20    7
EUCLID                                      0x0004   60    8
SYDNEY                                      0x0004   60    7
CALERN                                      0x0004   20    8
CD_ROM                                      0x0004   20    9
NYC1                                        0x0004   60    8
```

8. **To test the service's connectivity to the router, enter the following Technician Interface script command:**

    show ipx ping *<service_name>*

Example

```
$show ipx ping NW312_LOTUS

IPX Ping command, by name
-------------------------
Searching for NW312_LOTUS in server database.
Server NW312_LOTUS found, sending ping...
pinging NW312_LOTUS at 0x00000986.0x000000000001
IPX ping: 0x00000986.0x000000000001 is alive
```

Troubleshooting OSI

This section assumes that you have isolated a problem to OSI. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot OSI as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for OSI running on the slots in question.**

    The Technician Interface command is

    log -fftwid -eOSI -s<i><slot_no.></i>

    Example

    If you are filtering events from Slots 3 and 4, you enter

    log -fftwid -eOSI -s3 -s4

2. **Enter the following command and parameters to request data from the OSI interface:**

    osidata -s<i><slot no.></i> **-t**<i><type></i> **-i**<i><ID></i>

    <i><slot no.></i> is the number of a slot on which the OSI service is running on the router. Valid values are 1 to 13, inclusive.

    <i><type></i> is the database information you want displayed. Valid values are

    *   lsp_L1 — link state packet for Level 1
    *   lsp_L2 — link state packet for Level 2
    *   path_L1 — internal path control block for Level 1 path
    *   path_L2 — internal path control block for Level 2 path
    *   adj_L1 — adjacency control block for Level 1
    *   adj_L2 — adjacency control block for Level 2
    *   adj_ES — adjacency control block for end system

    <i><ID></i> is the identifier for the database information. The ID varies in length, depending on the type. For example, the LSP ID is 8 bytes, the adj ID is 6 bytes, and the path ID (also referred to as the router ID) is 6 bytes. All identifiers are in hexadecimal notation.

This command allows you to display OSI database information about an individual slot in the router. The display includes information about link state packets (LSPs), path control blocks, and adjacency control blocks.

The console displays the database information you requested or an error message.

For example, if you enter an **osidata -s 2 -t lsp_L1 -i aaaaaaaaaaaa0000** command to request a Level 1 LSP with the LSP ID aaaaaaaaaaaa0000 from the OSI service installed on Slot 2, and the OSI service responds to the request, the Technician Interface console displays messages similar to the following:

```
L2 LSPID aaaaaaaaaaaa0000
SRM_flags 0 0 0 0, SSN_flags 0 0 0 0, Ctrl flags 8
Lifetime 1200, Seqnum 2, Chksum 9b9a, Flags 03
01040349 0040020c 00148080 80aaaaaa aaaaaa01 0300080 8080aaaa
aaaaaaaa
```

If the OSI service cannot respond to the request for data, the console may display one of the following error messages:

- `Invalid slot number, can't parse cmd line`

  The slot does not exist.

- `Invalid ID, can't parse cmd line`

  You entered a number of bytes other than eight for the LSP ID.

- `No answer from called slot`

  The OSI service is not installed on the specified slot.

- `No data returned for ID message`

  An LSP does not exist for the specified ID on the specified slot.

- `Unknown database object type, can't parse cmd line`

  You entered an invalid value with the **-t** *<type>* option.

3. **To display the LSP ID, use the *osil1lsp* or *osil2lsp* alias, depending on the level (1 or 2).**

The alias definitions are

- osil1lsp = echo "L1 LSPDB"; get wfOsiL1LspHdrEntry.1

- osil2lsp = echo "L2 LSPDB"; get wfOsiL2LspHdrEntry.1

4. **To display the dynamic adjacency ID, use the *osiadjs* alias.**

The alias definition is

osiadjs = echo "Dynamic Adjacencies"; get wfOsiDynAdjEntry.9

5. **To display the path or router ID, use the *osil1routes* or *osil2routes* alias, depending on the level (1 or 2).**

The alias definitions are

- osil1routes = echo "L1 Fwd Routes"; get wfOsiL1RouteEntry.1

- osil2routes = echo "L2 Fwd Routes"; get wfOsiL2RouteEntry.1

Troubleshooting Switched Services

This section assumes that you have isolated a problem to the switched services. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot switched services as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the modem interface and PPP entities running on the slots in question.**

The Technician Interface command is

log -fftwid -eMODEMIF -ePPP -s<slot_no.>

Example

If you are filtering events from Slots 3 and 4, you enter

log -fftwid -eMODEMIF -ePPP -s3 -s4

2. **Inspect the log as follows:**

   a. **If the connection is V.25bis, make sure that the modem sent the call request number (CRN).**

   b. **Make sure the telephone number is correct.**

   If the modem sent the CRN, the telephone number is correct, and the modem did not dial, check the cabling and configuration of the modem.

   c. **Determine how PPP is negotiating during the connection.**

For a successful connection, the control protocol on both sides of the configured demand circuits comes up, and the associated events appear in the log.

3. **Filter the log to display messages of all severity levels for the switched access services running on the slots in question.**

The Technician Interface command is

log -fftwid -eSWSERV -s<slot_no.>

Example

If you are filtering events from Slots 3 and 4, you enter

log -fftwid -eSWSERV -s3 -s4

4. **Determine whether the circuit is in slave mode or master mode.**

5. **Filter the log to display the network-layer protocol event messages and determine whether or not they are coming up.**

6. **Use the Technician Interface get command or the Statistics Manager Quick Get tool to examine the following MIB objects for configuration settings and errors:**

   — wfPppCircuitEntry

   — wfPppLine Entry

   — wfPPPWhoamiEntry

   — wfSwservOptsEntry

   — wfSwservOutPhoneNumEntry

   — wfModemIfEntry

7. **If you are running IP, and RIP or OSPF, for dial backup, do the following:**

   a. **Ping across the connection from the primary line.**

      If the ping fails, and the router fails to establish a backup connection, issue the Technician Interface **show ip arp** script command. Determine whether you statically configured the ARP cache. If you are running Frame Relay on the primary line, configure an IP adjacent host.

   b. **Check the slave site's routing table for the routes it learned from the master site. Do the same when the backup line comes up.**

Refer to one of the following sections, if it applies to the problem:

- "Master Cannot Connect to Slave"
- "Troubleshooting RS232 Raise DTR Dial (Unbalanced)"
- "Troubleshooting V.35 Raise DTR Dial (Balanced)"
- "Troubleshooting ISDN BRI and PRI"

Master Cannot Connect to Slave

In a dial backup application, if the master side cannot make the connection to the slave side, do the following:

1. **Make sure the configuration file is correct.**

2. **If the connection is V.25bis, check the log for the CRN.**

3. **Try reversing the master and slave.**

4. **Make sure that you enabled BOFL on the primary link.**

If you can establish this connection, recheck the configuration of the modem and router.

Troubleshooting RS232 Raise DTR Dial (Unbalanced)

If DTR is up on the backup circuit (the master end), causing the backup modem to dial even though the primary line is up, do the following:

1. **Verify whether the modem is sending a DSR (data set ready) signal to the router interface in the on state (positive voltage) when the local and remote modems are not connected.**

   If it is, configure the modem for DSR to follow CD (Carrier Detect), or configure DSR to be in the off state until the modem receives a DTR (data terminal ready) signal. Unfortunately, DCE manufacturers use inconsistent terminology for these settings.

   When the router detects that DSR is in the on state (that is, receiving positive voltage), it brings DTR high regardless of the state of the primary line. This in turn causes the modem to dial. If the router does not see any DSR (0 voltage), the router will also bring DTR high. This in turn causes the modem to dial.

2. **If the router's connection to the modem is a 44-pin synchronous interface, and the modem is a master, make sure the modem can send the RI (ring indicator) signal from Pin 22 to the router interface in the control off state (negative voltage).**

   Most RS232 modems support this control signal. If the modem does not support this control signal, use the Configuration Manager to edit the connector of the backup line, click on Modem, and disable ring indicator.

   The RS232 pin assignments are

   - RI (ring indicator) Pin 22
   - DCD (data carrier detect) Pin 8
   - DTR (data terminal ready) Pin 20
   - DSR (data set ready) Pin 6

Troubleshooting V.35 Raise DTR Dial (Balanced)

If the DTR is up when it should not be, causing the modem or CSU to initiate a dial sequence, do the following:

1. **If the router's connection to the modem or CSU is a 44-pin synchronous interface, and the modem is a master, make sure the modem or CSU can send the RI signal from Pin J to the router interface in the control off state.**

   Some CSUs do not support the Pin J, RI signal. If the modem or CSU does not support this control signal, use the Configuration Manager to edit the connector of the backup line, click on Modem, and disable ring indicator.

   If the CSU does not supply RI Pin J, you can create a custom cable to use another signal, such as RLSD (received line signal detection) pin F, as RI Pin J. RLSD is typically low until the modem establishes a connection, and goes low again after DTR toggles.

➡ **Note:** *Disabling ring indicator on the router has no effect in this case. The absence of the RI control signal at the master end causes DTR to go high.*

2. **Disconnect the local and remote CSUs from the DCE, and use a breakout box to verify whether the DCE (modem or CSU) is sending a DSR (data set ready) signal to the router interface in the on state (positive voltage).**

If it is, configure the DCE for DSR to follow CD, or configure DSR to be in the off state until the DCE receives a DTR signal, and reconnect the CSUs. Unfortunately, DCE manufacturers use inconsistent terminology for these settings.

➡️ **Note:** *This is the preferred way to resolve this problem. However, if the CSUs do not support this solution, use the Configuration Manager to edit the connector of the backup line, click on modem, and disable the ring indicator. DTR then goes high only if the primary line becomes unavailable.*

The V.35 pin assignments are

- RLSD (received line signal detect) Pin F

- RI (ring indicator) Pin J

- DSR (data set ready) Pin E

- DTR (data terminal ready) Pin H

Troubleshooting ISDN BRI and PRI

Troubleshoot ISDN BRI and PRI as follows:

1. (ISDN PRI only) Verify that MCT1/MCE1 initialized correctly.

   Example

```
# 7: mm/dd/yy 10:38:39.363   DEBUG   SLOT  4  DS1E1  Code:  50
Connector COM1, Logical Line 1 time_slot = 16.
Connector COM1, Logical Line 1 time_slot = 17.
Connector COM1, Logical Line 1 time_slot = 18.
Connector COM1, Logical Line 1 time_slot = 19.
Connector COM1, Logical Line 1 time_slot = 20.
Connector COM1, Logical Line 1 time_slot = 21.
Connector COM1, Logical Line 1 time_slot = 22.
Connector COM1, Logical Line 1 time_slot = 23.
Connector COM1, Logical Line 1 time_slot = 24.
Connector COM1, Logical Line 1 initialization complete
```

2. Filter the log to display messages of all severity levels for the ISDN, ISDN BRI, and switched access services running on the slots in question.

The Technician Interface command is

log -fftwid -eISDN -eISDN_BRI -eSWSERV -s*<slot_no.>*

Example

If you are filtering events from Slots 3 and 4, you enter

log -fftwid -eISDN -eISDN_BRI -eSWSERV -s3 -s4

3. **Refer to the log to verify that**

- Layer 2 and Layer 3 of ISDN started.

    ### *Example*

    ```
    # 21: mm/dd/yy 03:16:08.283  TRACE  SLOT  1  ISDN  Code:  16
    Starting Layer 3.
    # 22: mm/dd/yy 03:16:08.286  TRACE  SLOT  1  ISDN  Code:  13
    Starting Layer 2.
    ```

- The Line Manager initialized.

    ### *Example*

    ```
    # 3: mm/dd/yy 03:15:49.393  INFO   SLOT  1  SWSERV  Code:  65
    Line Manager Initializing.
    ```

- The basic rate interface (BRI) digital subscriber loops (DSLs) become active.

    ```
    Example
    # 2: mm/dd/yy 03:15:42.755  INFO  SLOT  1  ISDN_BRI  Code:  8
    ISDN BRI2, DSL 0, Interface enabled.
    ```

- ISDN assigns the terminal endpoint identifiers (TEIs).

    ### *Example*

    ```
    # 31: mm/dd/yy 03:16:10.541  INFO  SLOT  1  ISDN     Code:  4
    TEI 64 assigned on DSL 0.
    ```

- (ISDN BRI in N. America only) The switched access service (SWSERV) entity registers one or more Service Profile Identifiers (SPIDs).

    ### *Example*

    ```
    # 30: mm/dd/yy 03:16:10.439  INFO  SLOT  1  SWSERV  Code: 102
    Sending Registration for SPID1:4002 on DSL 0.
    ```

- The ISDN configuration includes the correct switch type.

    ### *Example*

    ```
    # 11: mm/dd/yy 03:15:49.517  INFO  SLOT  1  SWSERV  Code: 136
    ISDN Configured for switch type BRI NI1.
    ```

4. **Look at the attribute values of the following MIB objects:**

- wfIsdnSwitchCfgEntry

- wfPppCircuitEntry

- wfSwservOptsEntry

- wfPppLineEntry

- wfIsdnBriInterfaceEntry

- wfPppWhoamiEntry

- wfSwservOutPhoneNumEntry

- wfIsdnLocalPhoneNumEntry

- wfIsdnPoolEntry

- wfIsdnCallInfoEntry

If a call fails, do the following:

1. **Verify that a line is available from a pool to make a call.**

2. **Verify that a call setup is in the log and that the calling and called number are correct.**

3. **If the ISDN connection is present, filter the PPP event messages to verify that the PPP negotiation succeeded. To do this from the Technician Interface, enter**

   log -ePPP -ffdwit

4. **Verify that the CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) data in the wfSwservOptsEntry matches that of the remote router's wfPppWhoamiEntry.**

   If it is CHAP, make sure the Secret is identical on both sides of the link.

5. **Verify that the protocol network numbers and adjacent host information are correct.**

6. **If using call screening on incoming calls, verify that the numbers in the Dialup➜Incoming Phone Numbers table match those in the Call Setup messages received.**

Troubleshooting Other Networking Protocols

This section assumes that you have isolated a problem to a network protocol. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot network-layer protocols not mentioned previously in this chapter as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the protocol in question.**

    The Technician Interface command is

    log -fftwid -e<ENTITY> **-s**<slot_no.>

    When specifying the <ENTITY>, use uppercase letters. Refer to *Event Messages for Routers and BNX Platforms* for a list of the entities.

    ### Example

    If you are filtering events from the XNS entity running in Slots 3 and 4, you enter

    log -fftwid -eXNS -s3 -s4

2. **Check the base records.**

    For example, if the networking software with which you are having a problem is XNS, enter **get wfXnsBase.*.0** to check the status of the XNS software.

    The most important attributes are

    *   The State attribute shows whether the protocol is up (1), down (2), initializing (3), or not present (4).

        You cannot change this setting.

    *   The Create or Delete attribute reveals whether the network software is created (1) or deleted (2).

    *   The Enable or Disable attribute reveals whether the protocol is enabled (1) or disabled (2).

3. **Check the values of the following statistics twice and compare them to determine whether the protocol is currently receiving and transmitting packets, and generating errors:**

   • The reception and transmission statistics

     If the reception or transmission statistics do not change, do the following:

     — Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.

     — Try disabling and enabling the protocol, and watch the log messages to determine why the connection will not come up.

   • The error statistics

4. **Make sure that the next hop and network you are trying to reach are in the routing table entries.**

5. **Verify the configuration parameters.**

6. **Use Packet Capture and a network analyzer to check the segments involved in the problem.**

Chapter 7
Troubleshooting a Site Manager Problem

This chapter describes how to solve Site Manager problems. It includes the following sections:

- "<u>Site Manager Won't Start</u>"

- "<u>Cannot Establish a Site Manager Session with the Router</u>"

- "<u>Target Does Not Respond (or Similar Message)</u>"

- "<u>Cannot Allocate Colormap Message</u>"

- "<u>UNIX Workstation Generating Core Dumps</u>"

Site Manager Won't Start

The following sections describe how to troubleshoot a Site Manager installation:

- "<u>Site Manager Won't Start on a PC</u>"

- "<u>Site Manager Won't Start on a UNIX Workstation</u>"

Site Manager Won't Start on a PC

Refer to the section that applies to your problem:

- "<u>Cannot Find File Message</u>"

- "<u>Working Directory or Path Is Invalid Message</u>"

- "<u>Unable to Find UDP Port Numbers for SNMP Message</u>"

Cannot Find File Message

If a message like the one in Figure 7-1 states that the application cannot find the WFSM.EXE or WINSOCK.DLL (Windows Socket Dynamic Link Library) files when you click on the PC/Site Manager icon, install, configure, and test the TCP/IP communication stack.

Figure 7-1. Cannot Find File Error Message

➡ **Note:** *You must install a TCP/IP stack such as Chameleon or Distinct TCP/IP and configure it properly before you install Site Manager.*

Test the TCP/IP stack as follows:

1. **Use the TCP/IP communication stack on the PC to ping the interface on the PC's network interface card.**

   If you cannot ping the interface, configure the TCP/IP stack.

2. **Use the TCP/IP communication stack on the PC to ping another node on the local network.**

   If you do not receive a response to the ping request, do the following:

   a. **Check the cable connection to the PC.**

   b. **Check the cable connection to the local node you are trying to ping.**

   c. **Make sure that you configured the TCP/IP stack.**

      If you cannot ping a device that can ping other devices, and the cabling is OK, the configuration of the TCP/IP stack is incorrect.

3. **Make sure that the environment variable PATH contains only the path to the protocol stack that you want Site Manager to use.**

   Otherwise, the PC will boot, but Site Manager may use the wrong protocol stack; it uses the first winsocket library it finds when searching the directories in the environment variable PATH.

Working Directory or Path Is Invalid Message

These messages appear when the properties of the PC (personal computer) Site Manager icon fail to match the installation and configuration. Do the following:

1. **Click the PC/Site Manager icon.**

2. **Select File➤Properties.**

   The Program Item Properties window appears.

3. **Make sure the settings in the Command Line and Working Directory match the directory of the *WFSM.EXE* and configuration files.**

Unable to Find UDP Port Numbers for SNMP Message

The *SERVICES* file is in

- The *NETMANAG* directory if you are using Chameleon.

- The *ETC* directory if you are using Distinct TCP/IP.

Make sure the *SERVICES* file contains the following lines:

```
snmp_trap      162/udp
snmp           161/udp
```

Site Manager Won't Start on a UNIX Workstation

If you are having problems starting Site Manager, do the following:

1. **Verify that the workstation meets all of the minimum system requirements.**

2. **Enter the wfchkenv command to verify that the path variables and environment variables are set up correctly.**

   Make sure the link */usr/wf* points to the directory where you installed Site Manager.

3. **Enter the wfchkinst command to verify the installation.**

4. **Verify that you updated the *$/etc/services$* file correctly, as follows:**

   • If the workstation running Site Manager is accessing NIS (Network Information Services), update the *$/etc/services$* file on the workstation that is providing NIS.

   • If the workstation running Site Manager is not accessing NIS, update the *$/etc/services$* file on the local workstation.

5. **Verify that no two processes bind to the same SNMP trap port number.**

   For example, Site Manager and Sun Net Manager cannot both bind to the SNMP trap port.

6. **Refer to one of the following sections if it applies to your problem:**

   • "Unable to Load SNMP MIB or File Was Inaccessible Message"

   • "Unable to Run . . . Module Message"

Unable to Load SNMP MIB or File Was Inaccessible Message

If messages like the following appear, add swap space to your workstation:

```
wfsm: unable to load the SNMP MIB (c3202)
wfsm: The SNMP MIB could not be loaded from the file
/usr/wf/lib/WFMIB.defs
Either the file was inaccessible, or not enough memory to load file
```

Unable to Run . . . Module Message

Before starting Site Manager, make sure that you are in a directory for which you have write permission. If you start Site Manager in a directory where you do not have write access, you will not be able to start the Site Manager tools. A message such as Unable to Run Configuration Module appears.

Cannot Establish a Site Manager Session with the Router

If the connection to the router fails to establish, do the following:

1. **Make sure the IP address in the Router Connections window matches the IP address of the router.**

2. **Increase the timeout and retries settings and retry.**

3. **Make sure that the IP address of the Site Manager workstation is within the list of the router's community managers.**

   You can do this by using another Site Manager workstation or by using the Technician Interface. Refer to one of the following sections:

   • "Using an Alternative Site Manager Workstation to Enable Access"

   • "Using the Technician Interface to Enable Access"

   • "Cannot Connect after Upgrading a Series 5 Router"

   • "Cannot Connect Site Manager Running on a PC"

   • "Cannot Connect Site Manager Running on a UNIX Workstation"

   • "Cannot Allocate Colormap Message"

Using an Alternative Site Manager Workstation to Enable Access

Enable SNMP access as follows:

1. **Access a workstation that allows you to connect to the router.**

2. **Start the Configuration Manager in dynamic mode.**

3. **Select Protocols➔IP➔SNMP➔Communities.**

   The SNMP Community list appears.

4. **Select Community➔Managers.**

5. **If the manager list does not contain the IP address of the Site Manager workstation that failed, select Manager➔Add Manager and add it.**

Using the Technician Interface to Enable Access

Enable SNMP access as follows:

1. **Enter the following Technician Interface command:**

   get wfSnmpMgrEntry.4.*

   The following line appears for each workstation configured as an SNMP manager:

   ```
   wfSnmpMgrEntry.wfSnmpMgrName.<community index>.<IP address> = (nil)
   ```

   An IP address of 0.0.0.0 allows any workstation to become an SNMP manager.

2. **If the manager name list does not contain the IP address of the Site Manager workstation that failed, assign one.**

3. **Try again to establish an IP connection with the router.**

Cannot Connect after Upgrading a Series 5 Router

After upgrading from Series 5 software to Series 7 or higher, you must first boot the router with the *TI.CFG* file and execute the **backplane FN** command for an FN (Feeder Node) or AFN (Access Feeder Node), **backplane LN** command for an LN (Link Node) or ALN (Access Link Node), or **backplane CN** command for a CN (Concentrator Node) to prepare the backplane to run the router software. You must then reboot the router.

For detailed instructions, refer to the *Upgrading Routers from Version 5 to Version 10.0* guide.

Cannot Connect Site Manager Running on a PC

Troubleshoot Site Manager connectivity failures on a PC as follows:

1. **Use Distinct or Chameleon to ping the local router interface.**

   If you cannot ping the router, Site Manager will not communicate with it.

   If the ping attempts fail, and the number of transmitted requests and reply counters fail to increment, the PC did not receive a response to the ARP request for the router's MAC address. Do the following:

   a. **Check the configured address of the PC, the subnet mask, and the gateway.**

b. **Try to use Distinct or Chameleon to ping other stations on the LAN.**

c. **Try to ping the router port from other PCs or workstations on the LAN.**

   If the ping attempts fail, but the number of transmitted requests increments, the PC has a path to the requested address, but failed to receive a response. Do the following:

d. **Verify that the router interface has a path to the PC.**

e. **Verify that the segment on which the PC is located does not contain duplicate IP addresses.**

f. **Issue the Technician Interface get wfIpInterfaceEntry.45.* command to display the number of ICMP echo requests the interface received for that IP address.**

2. **After the PC can ping the local router interface and receive a response, ping another interface on the router to determine whether the end node knows how to get off the local network. If this test fails, check the subnet mask and default gateway definitions on the PC.**

Cannot Connect Site Manager Running on a UNIX Workstation

Troubleshoot Site Manager connectivity failures on a UNIX workstation as follows:

1. **Log into an account from which you can run Site Manager.**

2. **Use the command line interface of the workstation to ping the local router interface.**

   If this fails, and the number of transmitted requests and reply counters fail to increment, the workstation did not receive a response to the ARP request for the router's MAC address. Do the following:

a. **Check the configured address of the workstation and its subnet mask.**

b. **Try to use the command line interface to ping other stations on the LAN.**

c. **Try to ping the router port from other PCs or workstations on the LAN.**

If the ping attempts fail, but the number of transmitted requests increments, the workstation has a path to the requested address, but failed to receive a response. Do the following:

a. **Verify that the router interface has a path to the PC.**

b. **Verify that the segment on which the workstation is located does not contain duplicate IP addresses.**

c. **Issue the Technician Interface get wfIpInterfaceEntry.45.* to display the number of ICMP echo requests the interface received for that IP address.**

3. **After the workstation can ping the local router interface and receive a response, ping another interface on the router to determine whether the end node knows how to get off the local network. If this test fails, check the routing table on the UNIX workstation.**

Target Does Not Respond (or Similar Message)

The destination node of the ping request failed to respond. To determine whether the pinged node is in the local ARP cache, issue the **arp -a** command. Most UNIX workstations display the current ARP cache in response to this command.

If the MAC address of the station pinged unsuccessfully is in the ARP cache, check the pinged interface's wfIpInterfaceEntry statistics.

If the MAC address is not in the ARP cache, do the following:

1. **Enter the following command to check the workstation's interface definition:**

   ifconfig -a

   The workstation displays all of the assigned IP addresses and subnet masks.

2. **From other nodes on the segment, ping the router's interface.**

3. **From other nodes on the segment, ping the workstation from which you are trying to establish a Site Manager connection.**

Cannot Allocate Colormap Message

The Site Manager cannot allocate any colors for its display because another process on the SPARCstation is using them. Set the background to a single color or terminate some other background process.

UNIX Workstation Generating Core Dumps

Separate one core dump into smaller files and send them to the Bay Networks Technical Response Center as follows:

1. **Issue the gdb -c core command.**

   This command fails if you do not specify the name of an executable file, but the path and name of the file that was executing appears.

2. **Issue one of the following commands:**

   gdb -c core *<pathname>*

   or

   gdb *<pathname>* **core**

   <pathname> is the path and name of the executable file displayed in Step 1.

3. **Refer to Chapter 8 for instructions on how to send the files to the Bay Networks Technical Response Center.**

Chapter 8
Getting Help

This chapter includes the following sections:

- "Reporting a Problem to the Bay Networks Technical Response Center"

- "Sending and Retrieving Files to and from Bay Networks"

Reporting a Problem to the Bay Networks Technical Response Center

This section identifies the information we need when you call to report a problem.

Prepare to answer the following questions to help us expedite a solution to your problem:

1. **What is the site ID?**

   This number allows us to track your problem and look up other related problems for the site having the problem. It also allows us to do a case history of the router(s) in question.

2. **What is the Service Contract Type?**

3. **What is the router's serial number?**

   Enter the Technician Interface **get wfHwBase.3.0** command to display it. Or, use the Quick Get tool to display wfHardwareConfig➤wfHwBase➤ wfHwBpSerialNumber.

4. **What are the symptoms of the problem?**

5. **What workaround are you using?**

6. **When did the problem start occurring?**

7. **Under what conditions does the problem occur?**

8. **What, if anything, has changed in the router and/or network?**

9. **Can you reproduce the problem, and if so, how?**

10. **How is the problem affecting your network?**

11. **What revision of software is currently installed?**

12. **Does the log show you any additional information?**

13. **Do you have a trace of the problem?**

14. **Can you send the Bay Networks Technical Response Center a copy of the configuration file and a binary version of the log file?**

    Go to the next section for instructions.

15. **Can we dial into the router and use Telnet to access it in order to troubleshoot the problem?**

16. **If we do not have an up-to-date diagram of your network, can you fax it to us?**

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-0052

Sending and Retrieving Files to and from Bay Networks

Sending us your configuration files, traces, and router logs can help us isolate and solve the problem with your router. You can send files to and from Bay Networks by using one of the following methods:

•   Use the Bay Networks anonymous FTP file server.

    If you can access the Internet, you can use FTP to forward configuration files, traces, router logs, and so on.

•   Use an asynchronous file transfer program such as Procom.

•   Connect a modem to the problem router and ask us to use XMODEM commands to retrieve configuration files, logs, and traces.

- Fax copies to the Bay Networks Technical Response Center at: (508)-670-8765

➡️ **Note:** *Although Bay Networks has a bulletin board system available to contracted support customers, you cannot transfer files over it.*

Use the Bay Networks anonymous FTP file server as follows:

1. **Enter the following command:**

    ftp 192.32.253.5

2. **Enter the following after the Name prompt:**

    anonymous

3. **Enter the following after the Password prompt.**

    ident

4. **To send a file, enter cd incoming; to retrieve a file, enter cd outgoing.**

5. **If your company does not have a dedicated directory, enter the following command to create one:**

    mkdir *<your_company_directory_name>*

6. **Enter the following command to access your company directory:**

    cd *<your_company_directory_name>*

7. **Enter the following command to specify a binary transmission:**

    bin

8. **Enter put** *<filename>* **if you are sending a file, or get** *<filename>* **if you are retrieving a file.**

9. **When a message indicates that a successful binary transmission occurred, enter the quit command to exit the FTP session.**

Appendix A
Reading the Event Log

This appendix provides examples and explanations of the descriptive text in event messages, including debug messages. It includes the following sections:

- "System Startup"

- "Dial-on-Demand Raise DTR Log"

- "Dial-on-Demand V.25bis"

- "MCT1 Log Information in a Lab Testing Environment"

Refer to the *Configuring ATM Services* manual for sample ATM events.

→ **Note:** *To promote readability, this appendix does not show redundant messages or those that do not pertain to the topic.*

This appendix does not identify the components of an event. Refer to *Event Messages for Routers and BNX Platforms* for this information.

System Startup

The following sample message is from a log of a Series 7 router after we restarted it by entering the **boot 2:- 2:log.cfg** command. This message indicates that the system is preparing the router software image:

```
@ 29:  mm/dd/yy  11:48:14.507  DEBUG # 2        BOOT ( 12)  Image is in
compressed format... decompressing
```

The boot PROM generates the following message for each slot. This message shows the revision of the boot PROM on the FRE processor module, *not* the revision of software.

```
@ 12:  mm/dd/yy  11:47:57.007  INFO # 3        GAME ( 11)  Starting image
rel/<revision_no.>/boot Day MMM DD 00:12:43 EDT yyyy
```

Because the router received instructions to perform a named boot (that is, it received instructions to boot with a specified router software image or configuration file on a specified slot, Slot 2), the system does *not* query the backplane for the router software image; Slot 2 becomes the server of the router software image.   The router bootstraps the loader software and loads the router software image (in this example, *bn.exe)* from the memory card in Slot 2.

```
@ 25:  mm/dd/yy  11:48:06.058  DEBUG # 3        GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
+ LOADER: starting gate 0x0000e @ 0x3050ced2 (env=0x00000000,
flags=0x00000001)
@ 26:  mm/dd/yy  11:48:08.054  DEBUG # 2        GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
+ LOADER: starting gate 0x0000e @ 0x3050ced2 (env=0x00000000,
flags=0x00000001)
@ 27:  mm/dd/yy  11:48:12.695  DEBUG # 2        NVFS ( 37)  Memory Card
Inserted: FLASH (EMBEDDED ALGORITHMS) Memory Type Detected
+ Flash media info: Mfg ID 0x1, Device ID 0x29, number of chips 8
@ 28:  mm/dd/yy  11:48:12.695  DEBUG # 2        BOOT (  6)  Found image
'bn.exe' on local file system... booting
@ 29:  mm/dd/yy  11:48:14.507  DEBUG # 2        BOOT ( 12)  Image is in
compressed format... decompressing
```

FSM (finite state machine) messages indicate slot-to-slot communication. Each slot is in one of four different states: "DOWN," "SYNC," "ACTIV" (active), and "HOLD."

Each slot transmits BOFL requests via the backplane to the other slots in the router in order to determine which slots are active. Each slot transmits 16 BOFL requests per second. The operating system logs the status of each slot as follows:

- If a slot does not hear from a remote slot within 4 seconds (s) (64 BOFL requests), it logs the state of that slot as "DOWN."

- If a slot receives some BOFL responses from a remote slot, or does not receive all that it should have, it logs the state of that slot as "SYNC."

- If a slot receives all of the necessary BOFL responses from a remote slot that it previously determined as "DOWN" or "SYNC," it logs a message stating that the remote slot is "reconnected" to the backplane.

For example, in Message 40, Slot 3 declares that Slot 2 is back up.

```
@ 30:  mm/dd/yy  11:48:19.153  DEBUG # 3       GAME ( 74)  @REMOTE  2
FSM:  FLOW ->  HOLD (00014a: TIME-OUT -- last=0000f6)
@ 31:  mm/dd/yy  11:48:19.153  WARN # 3        GAME (  8)  slot  2 became
disconnected
@ 32:  mm/dd/yy  11:48:21.273  DEBUG # 2       GAME ( 73)  @REMOTE  3
FSM:  FLOW -> ACTIV (0000f9: 90000007 00012d 20000000 00000000)
+ @REMOTE  3 FSM: ACTIV ->  DOWN (0000f9: 90000007 00014d 00000000
20000000)
@ 33:  mm/dd/yy  11:48:21.273  WARN # 2        GAME (  8)  slot  3 became
disconnected
@ 34:  mm/dd/yy  11:48:21.343  DEBUG # 2       GAME ( 73)  @REMOTE  3
FSM:  DOWN ->  SYNC (0000fa: 90000007 000171 00000000 00000000)
@ 35:  mm/dd/yy  11:48:21.386  DEBUG # 2       GAME ( 73)  @REMOTE  3
FSM:  SYNC -> ACTIV (0000fb: 90000006 000172 20000000 20000000)
@ 36:  mm/dd/yy  11:48:21.386  INFO # 2        GAME ( 10)  slot  3 became
re-connected
@ 37:  mm/dd/yy  11:48:21.602  DEBUG # 3       GAME ( 73)  @REMOTE  2
FSM:  HOLD ->  DOWN (000171: a0000007 0000f9 00000000 00000000)
@ 38:  mm/dd/yy  11:48:21.658  DEBUG # 3       GAME ( 73)  @REMOTE  2
FSM:  DOWN ->  SYNC (000171: a0000006 0000fa 10000000 10000000)
@ 39:  mm/dd/yy  11:48:21.860  DEBUG # 3       GAME ( 73)  @REMOTE  2
FSM:  SYNC -> ACTIV (000175: a0000007 0000fd 10000000 10000000)
@ 40:  mm/dd/yy  11:48:21.860  INFO # 3        GAME ( 10)  slot  2 became
re-connected
```

The router is loading the router software image.

```
@  41:  mm/dd/yy  11:48:22.269  DEBUG # 2      BOOT ( 13)  Image loaded,
jumping to: 0x30024000
@  42:  mm/dd/yy  11:48:26.007  INFO # 2      GAME ( 11)  Starting image
rel/9.00 Fri Jul 28 17:12:26 EST 1995
```

The software running in Slot 2 synchronized the system clock (WCLCK) with the other slots in the router.

```
@  43:  mm/dd/yy  11:48:25.265  DEBUG # 2       GAME (124)  WCLK set:
new=b1506bc9.84a00000 old=b1506bc9.44000000 rtc=b1506bca.00000000
```

+ WCLK set: err=00000000.00000000 cor=00000000.00000000
inc=00000000.00000000

Slot 2 is attempting to read the *log.cfg* configuration file specified in the boot command from the memory card in Slot 2. The NVFS (Non-Volatile File System) entity is responsible for reading and writing to the memory card.

```
@  57:  mm/dd/yy  11:48:34.314  DEBUG # 2       GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
@  58:  mm/dd/yy  11:48:34.318  DEBUG # 2     LOADER (  2)  Loader
starting service gate 0x000a1 @ 0x300a22ea (env=0x00004009, flags=0x1)
@  59:  mm/dd/yy  11:48:34.322  DEBUG # 2       GAME (200)  Board ID
Client: slot 2, type 2
@  60:  mm/dd/yy  11:48:34.439  DEBUG # 2     LOADER (  2)  Loader
starting service gate 0x00066 @ 0x30041692 (env=0x00004009, flags=0x1)
@  61:  mm/dd/yy  11:48:34.459  DEBUG # 2       NVFS ( 60)  Memory card
inserted: FLASH (EMBEDDED ALGORITHMS) memory type detected
+ Memory card media info: Mfg ID 0x1, Device ID 0x29, number of chips 8
@  62:  mm/dd/yy  11:48:34.459  INFO # 2       NVFS ( 42)  Service
initializing.
@  63:  mm/dd/yy  11:48:34.564  DEBUG # 2     LOADER (  2)  Loader
starting service gate 0x00013 @ 0x30095442 (env=0x00004009, flags=0x1)
@  64:  mm/dd/yy  11:48:34.564  DEBUG # 2        MIB ( 12)  Attempting to
obtain config file
@  65:  mm/dd/yy  11:48:34.564  DEBUG # 2       GAME ( 84)  FWD [ 2-0007]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
```

Slot 2 received a boot request from Slot 3.

```
@  66:  mm/dd/yy  11:48:34.658  DEBUG # 2       BOOT (  3)  Boot service
request received from 0x1000000e
```

Slot 2 is reporting that messages it sent to slot 3 were not acknowledged. Slot 3 is unable to respond because it is still booting.

The software interface to the kernel provides for the transmission of both unreliable and reliable messages. The two types of reliable messages are GFWD (GAME forward) and GRPC (GAME remote procedure call). Below is an example of a GFWD message failure logged by Slot 2.

```
@  67:  mm/dd/yy  11:48:34.701  DEBUG # 2        GAME ( 84)  FWD [ 2-0008]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
@  68:  mm/dd/yy  11:48:34.822  DEBUG # 2        GAME ( 84)  FWD [ 2-0009]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
@  69:  mm/dd/yy  11:48:34.955  DEBUG # 2        GAME ( 84)  FWD [ 2-000a]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
```

Slot 2 reads the configuration file *log.cfg*.

```
@  70:  mm/dd/yy  11:48:35.150  INFO  # 2        MIB (  4)  Using
configuration file '2:log.cfg'
@  71:  mm/dd/yy  11:48:35.221  DEBUG # 2        NVFS ( 63)  NVFS manager
is opening file 'log.cfg' for reading
@  72:  mm/dd/yy  11:48:35.271  DEBUG # 2        NVFS ( 64)  NVFS manager
is closing file 'log.cfg'
@  73:  mm/dd/yy  11:48:35.279  DEBUG # 2        MIB ( 66)  Initializing
MIB with configuration file information
@  74:  mm/dd/yy  11:48:35.354  INFO  # 2        MIB (  3)  Service
initializing.
@  75:  mm/dd/yy  11:48:35.377  DEBUG # 2        MIB ( 70)  Config manager
loading a 7.60 type configuration.
```

A soloist is a software entity that runs on only one slot in the router at a time. The soloists Technician Interface and TI_RUI (the remote command line interpreter) are starting up and determining what slot they run on (the election process). The gate ID for the Technician Interface is 0x15. The gate ID for TI_RUI is 0x57.

```
@  76:  mm/dd/yy  11:48:35.393  DEBUG # 2        LOADER (  2)  Loader
starting service gate 0x0000c @ 0x3003a926 (env=0x00000000, flags=0x1)
@  77:  mm/dd/yy  11:48:35.393  DEBUG # 2        GAME ( 23)  SOLO
(0x00015): election opening 30000000/30000000 (30000000) vote=00000000
@  78:  mm/dd/yy  11:48:35.424  DEBUG # 2        MIB ( 61)  D/A: Loaded
13 MIB mappings.
@  79:  mm/dd/yy  11:48:35.506  DEBUG # 2        GAME ( 97)  SOLO
(0x00015): election WON 0x20000000 (repl=b0000009/30000000)
@  80:  mm/dd/yy  11:48:35.510  DEBUG # 2        GAME ( 23)  SOLO
(0x00015): election CLOSING 30000000/30000000 (30000000) vote=00000000
@  81:  mm/dd/yy  11:48:35.533  DEBUG # 2        LOADER (  2)  Loader
starting service gate 0x0001e @ 0x300a1fa2 (env=0x00000000, flags=0x1)
@  82:  mm/dd/yy  11:48:35.541  INFO  # 2     NOV_SYNC (  2)  Service
initializing.
@  83:  mm/dd/yy  11:48:35.584  DEBUG # 2        GAME ( 97)  SOLO
(0x00015): election CLOSED 0x20000000 (repl=b0000009/30000000)
```

```
@  84:  mm/dd/yy  11:48:35.662  DEBUG # 2      LOADER (  2) Loader
starting service gate 0x04016 @ 0x30039a2e (env=0x00000000, flags=0x1)
@  85:  mm/dd/yy  11:48:35.732  DEBUG # 2         BOOT (  3) Boot service
request received from 0x1000000e
@  86:  mm/dd/yy  11:48:35.740  DEBUG # 2          GAME ( 23) SOLO
(0x00057): election opening 30000000/30000000 (30000000) vote=00000000
@  87:  mm/dd/yy  11:48:35.783  DEBUG # 2      LOADER (  2) Loader
starting service gate 0x00050 @ 0x30058392 (env=0x00000000, flags=0x1)
@  88:  mm/dd/yy  11:48:35.877  DEBUG # 2          GAME ( 97) SOLO
(0x00057): election WON 0x20000000 (repl=b0000009/30000000)
+ SOLO (0x00057): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@  93:  mm/dd/yy  11:48:35.967  DEBUG # 2          GAME ( 97) SOLO
(0x00057): election CLOSED 0x20000000 (repl=b0000009/30000000)
```

Learning Bridge (LB) is initializing.

```
@  94:  mm/dd/yy  11:48:35.971  INFO  # 2           LB (  2) Service
initializing.
@  95:  mm/dd/yy  11:48:36.006  DEBUG # 2           LB ( 63) CCT 811521904
update gate initializing.
```

Slot 3 is loading the router software image from slot 2.

```
@  97: mm/dd/yy   11:48:36.050 DEBUG #3         BOOT  (21) Server on slot
2 chosen for BB boot transaction
@ 104:  mm/dd/yy  11:48:36.104  DEBUG # 3         BOOT ( 18) BB boot
transaction started:
+    start address 0x30024000, size 0x000c89e0, checksum 0x038D2F95
@ 105:  mm/dd/yy  11:48:36.179  DEBUG # 3         BOOT ( 17) Client is
dropping duplicate reply from server 0x2000000D
+  - server seq 0, client seq 4780
```

The statistic and alarm soloist (gate ID 0x95), and file system control soloist (gate ID 0x98) are electing which slots to run on.

```
@ 107:  mm/dd/yy  11:48:36.346  DEBUG # 2          GAME ( 23) SOLO
(0x00095): election OPENING 30000000/30000000 (30000000) vote=00000000
@ 108:  mm/dd/yy  11:48:36.361  DEBUG # 2          GAME ( 97) SOLO
(0x00095): election WON 0x20000000 (repl=b0000009/30000000)
+ SOLO (0x00095): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 109:  mm/dd/yy  11:48:36.361  INFO  # 2          STA (  5) Service
initializing.
@ 110:  mm/dd/yy  11:48:36.385  DEBUG # 2          GAME ( 97) SOLO
(0x00095): election CLOSED 0x20000000 (repl=b0000009/30000000)
@ 111:  mm/dd/yy  11:48:36.385  DEBUG # 2      LOADER (  2) Loader
starting service gate 0x00095 @ 0x300a0932 (env=0x00000000, flags=0x3)
```

```
@ 112:  mm/dd/yy  11:48:36.502  DEBUG # 2      LOADER (  2)  Loader
starting service gate 0x00074 @ 0x300a17b2 (env=0x00000000, flags=0x1)
@ 113:  mm/dd/yy  11:48:36.502  INFO  # 2          SYS (  3)  Service
initializing.
@ 114:  mm/dd/yy  11:48:36.510  WARN  # 2          SYS (  2)  No system
record configured, creating one.
@ 115:  mm/dd/yy  11:48:36.631  DEBUG # 2         GAME ( 23)  SOLO
(0x00098): election opening 30000000/30000000 (30000000) vote=00000000
@ 116:  mm/dd/yy  11:48:36.643  DEBUG # 2         GAME ( 97)  SOLO
(0x00098): election WON 0x20000000 (repl=b0000009/30000000)
@ 117:  mm/dd/yy  11:48:36.646  DEBUG # 2         GAME ( 23)  SOLO
(0x00098): election CLOSING 30000000/30000000 (30000000) vote=00000000
@ 118:  mm/dd/yy  11:48:36.658  DEBUG # 2         GAME ( 97)  SOLO
(0x00098): election CLOSED 0x20000000 (repl=b0000009/30000000)
```

Each slot loads only the configured board drivers and protocols. It queries the
router software image and loads the necessary code onto the requesting FRE.

```
@ 122:  mm/dd/yy  11:48:37.178  DEBUG # 2         NVFS ( 63)  NVFS manager
is opening file 'bn.exe' for reading
@ 123:  mm/dd/yy  11:48:37.217  DEBUG # 2       LOADER ( 30)  Image
qenet.exe loaded successfully from 2:bn.exe
@ 124:  mm/dd/yy  11:48:37.217  DEBUG # 2         NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 125:  mm/dd/yy  11:48:37.225  DEBUG # 2       LOADER ( 15)  Loader
starting application qenet.exe, address 0x30541a10, gate id = 0x00045
@ 127:  mm/dd/yy  11:48:37.252  INFO  # 2       MODULE (  7)  Service
initializing.
+ QENET I/O module is present.
```

IP loaded successfully and is initializing. IP indicates that is in "router" mode,
rather than "host only" mode (message 133).

```
@ 128:  mm/dd/yy  11:48:38.018  DEBUG # 2       LOADER ( 30)  Image ip.exe
loaded successfully from 2:bn.exe
@ 129:  mm/dd/yy  11:48:38.018  DEBUG # 2         NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 130:  mm/dd/yy  11:48:38.049  DEBUG # 2       LOADER ( 15)  Loader
starting application ip.exe, address 0x304e9770, gate id = 0x00048
@ 132:  mm/dd/yy  11:48:38.080  INFO  # 2           IP (  4)  Protocol
initializing
@ 133:  mm/dd/yy  11:48:38.092  DEBUG # 2           IP (  8)  IP Redirector
Mode: Router
```

Slot 3 successfully loaded the router software image from Slot 2 and is starting up.

```
@ 134:  mm/dd/yy  11:48:38.259  DEBUG # 3         BOOT ( 19)  BB boot
transaction completed!! Jumping to address 0x30024000
```

DECnet successfully loaded onto Slot 2 and is initializing.

```
@ 135:  mm/dd/yy  11:48:38.631  DEBUG # 2     LOADER ( 30)  Image drs.exe
loaded successfully from 2:bn.exe
@ 137:  mm/dd/yy  11:48:38.646  DEBUG # 2     LOADER ( 15)  Loader
starting application drs.exe, address 0x304d4eb0, gate id = 0x00054
@ 139:  mm/dd/yy  11:48:38.697  INFO  # 2     DECnet (  2)  Protocol
initializing.
```

The IP RTM (routing table manager) is setting a bit map to indicate what slots it is running on. Convert the hexadecimal number to binary format. Then read the bit string from left to right. The leftmost bit is always 1. The second leftmost bit is for Slot 1, the third for Slot 2, the fourth for Slot 3, and so on. A map change occurs whenever the IP RTM starts up or dies on another slot.

```
@ 140:  mm/dd/yy  11:48:38.885  DEBUG # 2         IP (  8)  RTM self map
old 49,  new a0000049
```

IPX successfully loaded onto Slot 2 and the router software image closed. The operating system opens and closes the router software image whenever it needs to read an executable component.

```
@ 141:  mm/dd/yy  11:48:39.428  DEBUG # 2     LOADER ( 30)  Image ipx.exe
loaded successfully from 2:bn.exe
@ 142:  mm/dd/yy  11:48:39.428  DEBUG # 2       NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
```

IPX initialized, and the IPX RTM (routing table manager) and IPX STM (server table manager) are starting up and setting the maps to indicate which slots they are running on. The configured IPX network number is 000000aa.

```
@ 143:  mm/dd/yy  11:48:39.447  DEBUG # 2     LOADER ( 15)  Loader
starting application ipx.exe, address 0x304afec0, gate id = 0x0006b
@ 144:  mm/dd/yy  11:48:39.471  DEBUG # 2        IPX ( 28)  IPX RTM up on
slot 2.
@ 145:  mm/dd/yy  11:48:39.471  INFO  # 2        IPX (  1)  IPX Protocol
initializing.
@ 146:  mm/dd/yy  11:48:39.479  DEBUG # 2        IPX ( 38)  IPX STM up on
slot 2.
@ 147:  mm/dd/yy  11:48:39.486  DEBUG # 2        IPX ( 41)  IPX STM self
map old 0000006E, new A000006E.
@ 149:  mm/dd/yy  11:48:39.518  DEBUG # 2        IPX ( 25)  IPX DARP  gate
for slot 2 is up.
@ 150:  mm/dd/yy  11:48:39.525  DEBUG # 2        IPX ( 40)  IPX RTM self
map old 0000006C, new A000006C.
@ 151:  mm/dd/yy  11:48:39.545  DEBUG # 2       NVFS ( 63)  NVFS manager
is opening file 'bn.exe' for reading
```

```
@ 152:  mm/dd/yy  11:48:39.564  INFO  # 2         IPX ( 42)  IPX ADD Nwif
cct 1 Network 00.00.00.aa
@ 153:  mm/dd/yy  11:48:39.568  INFO  # 2         IPX ( 43)  IPX Nwif from
MIB Active cct 1 Network 00.00.00.aa
+ IPX Network 00.00.00.aa mapped to cct 1
```

SNMP successfully loaded from the router software image and the SNMP gate
soloist SNMP_START elects which slot it will run on.

```
@ 154:  mm/dd/yy  11:48:39.752  DEBUG # 2         LOADER ( 30)  Image
snmp.exe loaded successfully from 2:bn.exe
@ 155:  mm/dd/yy  11:48:39.756  DEBUG # 2          NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 156:  mm/dd/yy  11:48:39.764  DEBUG # 2         LOADER ( 15)  Loader
starting application snmp.exe, address 0x304a86e0, gate id = 0x00019
@ 157:  mm/dd/yy  11:48:39.768  INFO  # 2          SNMP (  7)  Protocol
initializing.
@ 158:  mm/dd/yy  11:48:39.791  DEBUG # 2          SNMP ( 36)  Agent received
new community public, assigned index 1.
@ 159:  mm/dd/yy  11:48:39.811  DEBUG # 2          SNMP ( 38)  Agent received
new manager 0 for community index 1
@ 161:  mm/dd/yy  11:48:39.861  DEBUG # 2          SNMP ( 40)  Agent spawned
the Trap Manager.
@ 162:  mm/dd/yy  11:48:39.869  DEBUG # 2          GAME ( 23)  SOLO
(0x0001b): election opening 30000000/30000000 (30000000) vote=00000000
@ 163:  mm/dd/yy  11:48:39.869  DEBUG # 2          SNMP ( 24)  Trap Manager
initializing.
```

The driver for the Ethernet chip set (ILACC) loads onto Slot 2 and initializes.

```
@ 164:  mm/dd/yy  11:48:39.943  DEBUG # 2         LOADER ( 30)  Image
ilacc.exe loaded successfully from 2:bn.exe
@ 165:  mm/dd/yy  11:48:39.943  DEBUG # 2          NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 166:  mm/dd/yy  11:48:39.951  DEBUG # 2         LOADER ( 15)  Loader
starting application ilacc.exe, address 0x304a6100, gate id = 0x00040
@ 167:  mm/dd/yy  11:48:39.955  INFO  # 2        CSMACD (  9)  Service
initializing.
@ 168:  mm/dd/yy  11:48:39.994  INFO  # 2        CSMACD ( 11)  Connector
XCVR1 enabled.
@ 169:  mm/dd/yy  11:48:39.998  DEBUG # 2        CSMACD ( 18)  Connector
XCVR1 initialization complete
+    Environment address - 304e1a00
+    Line record address - 305390a4
+    Hardware map address - 305c5ce4
+    Receive descriptor ring - 80000800
+    Transmit descriptor ring - 80000c00
+    Initialization block - 80007000
+    Silicon revision - 5
```

Slot 3 is booting revision 9.00 of *bn.exe*.

```
@ 176:  mm/dd/yy  11:48:41.007  INFO  # 3      GAME ( 11)  Starting image
rel/9.00 Fri Jul 28 17:12:26 EST 1995
```

The transceiver on Slot 2, Connector 1, does *not* have SQE (signal quality error) enabled. It reports the absence of an SQE signal, even though it does not need it.

```
@ 193:  mm/dd/yy  11:48:45.018  WARN  # 2      CSMACD ( 7)  Connector
XCVR1 no SQE.
```

Data Path elects the circuit control gate for Circuit 1. Each circuit must have a circuit control gate.

```
@ 195:  mm/dd/yy  11:48:45.025  DEBUG # 2        DP ( 23)  Creating
Circuit 1 soloist with line GH 0x4082
@ 196:  mm/dd/yy  11:48:45.025  DEBUG # 2      GAME ( 23)  SOLO
(0x00401): election opening 30000000/30000000 (30000000) vote=00000000
@ 197:  mm/dd/yy  11:48:45.049  DEBUG # 2      GAME ( 97)  SOLO
(0x00401): election WON 0x20000000 (repl=b0000009/30000000)
@ 198:  mm/dd/yy  11:48:45.053  DEBUG # 2      GAME ( 23)  SOLO
(0x00401): election CLOSING 30000000/30000000 (30000000) vote=00000000
```

ARP successfully initializes on Circuit 1.

```
@ 199:  mm/dd/yy  11:48:45.057  INFO  # 2      ARP ( 1)  Service is up
on circuit 1
```

Data Path registers the ISAP (internal services access point) for ARP.   The protocol type for ARP is 0806; this type determines that the ARP traffic will go to the correct gate and code by the DP (Data Path).   The number preceding the protocol type indicates the packet format (1 = Ethernet type 2, 2 = 802.2, 3 = SNAP [Subnetwork Access Protocol] , 4 = Novell, and so on).   Data Path registers Ethernet Type II or SNAP ARP frames on Circuit 1. In this example, Data Path does not register the 802.2 ARP frame type. If Circuit 1 received an 802.2 ARP frame, ARP would not receive it; instead it would go to the learning bridge.

```
 @ 201:  mm/dd/yy  11:48:45.135  DEBUG # 2       DP ( 34)  ISAP 0x30806
registered on cct 1.
@ 202:  mm/dd/yy  11:48:45.140  DEBUG # 2       DP ( 34)  ISAP 0x10806
registered on cct 1.
@ 205:  mm/dd/yy  11:48:45.213  DEBUG # 2      ARP ( 3)  Arp Client
128.128.2.2 registered
```

Data Path always registers Ethernet and SNAP frames for IP. In this example, Data Path registers ISAPs on Circuit 1 for the following protocols: IP (Ethernet type 0800), IPX (Ethernet type 8137), and DECnet (Ethernet type 6003). The number preceding the protocol indicates the packet.

Notice how DECnet only registers one packet type, while two IPX packet types register. This is because two unique IPX networks, with different packet encapsulation types, are on Circuit 1.

```
@ 217:  mm/dd/yy  11:48:45.494  DEBUG # 2       DP ( 34)  ISAP 0x30800
registered on cct 1.
@ 218:  mm/dd/yy  11:48:45.518  DEBUG # 2       DP ( 34)  ISAP 0x10800
registered on cct 1.
@ 219:  mm/dd/yy  11:48:45.537  DEBUG # 2       DP ( 34)  ISAP 0x16003
registered on cct 1.
@ 222:  mm/dd/yy  11:48:45.592  DEBUG # 2       DP ( 34)  ISAP 0x38137
registered on cct 1.
@ 225:  mm/dd/yy  11:48:45.623  DEBUG # 2       DP ( 34)  ISAP 0x18137
registered on cct 1.
```

Slot 3 successfully boots and is attempting to load the configuration file from Slot 2.

```
@ 227:  mm/dd/yy  11:48:49.521  DEBUG # 3       GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
@ 228:  mm/dd/yy  11:48:49.525  DEBUG # 3    LOADER (  2)  Loader
starting service gate 0x000a1 @ 0x300a22ea (env=0x00006009, flags=0x1)
@ 229:  mm/dd/yy  11:48:49.529  DEBUG # 3       GAME (200)  Board ID
Client: slot 3, type 2
@ 230:  mm/dd/yy  11:48:49.529  DEBUG # 2       GAME (199)  Board ID
Server: slot 3, type 2
@ 231:  mm/dd/yy  11:48:49.537  DEBUG # 3       GAME (201)  Board ID
Client reply: slot 2, type 2
@ 232:  mm/dd/yy  11:48:49.646  DEBUG # 3    LOADER (  2)  Loader
starting service gate 0x00066 @ 0x30041692 (env=0x00006009, flags=0x1)
@ 233:  mm/dd/yy  11:48:49.771  DEBUG # 3    LOADER (  2)  Loader
starting service gate 0x00013 @ 0x30095442 (env=0x00006009, flags=0x1)
@ 234:  mm/dd/yy  11:48:49.771  DEBUG # 3       MIB ( 12)  Attempting to
obtain config file
@ 235:  mm/dd/yy  11:48:49.787  DEBUG # 3       MIB ( 64)  Getting
configuration from slot 2
@ 236:  mm/dd/yy  11:48:49.865  DEBUG # 2       MIB ( 15)  Serving
configuration to slot 0x90000013
@ 237:  mm/dd/yy  11:48:49.869  DEBUG # 2       MIB ( 16)  Finished
serving configuration to slot 0x90000013
```

```
@ 238:  mm/dd/yy  11:48:49.932  DEBUG # 3        MIB ( 13)  Received
configuration from remote slot 0xa0000011
@ 239:  mm/dd/yy  11:48:49.936  INFO  # 3        MIB (  3)  Service
initializing.
@ 240:  mm/dd/yy  11:48:49.959  DEBUG # 3        MIB ( 70)  Config manager
loading a 7.60 type configuration.
```

Slot 3 tries to start the Technician Interface and TI_RUI soloists, but because they are already running on Slot 2, the soloist elections fail (elections logged as "LOST").

```
@ 244:  mm/dd/yy  11:48:50.045  DEBUG # 3        GAME ( 97)  SOLO
(0x00015): election LOST 0xb0000000 (repl=b0000009/30000000)
+ SOLO (0x00015): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 245:  mm/dd/yy  11:48:50.072  DEBUG # 3        GAME ( 97)  SOLO
(0x00015): election CLOSED 0x10000000 (repl=b0000009/30000000)
@ 246:  mm/dd/yy  11:48:50.107  DEBUG # 3        GAME ( 23)  SOLO
(0x00057): election opening 30000000/30000000 (30000000) vote=00000000
@ 247:  mm/dd/yy  11:48:50.115  DEBUG # 3      LOADER (  2)  Loader
starting service gate 0x0001e @ 0x300a1fa2 (env=0x00000000, flags=0x1)
@ 248:  mm/dd/yy  11:48:50.115  INFO  # 3   NOV_SYNC (  2)  Service
initializing.
@ 249:  mm/dd/yy  11:48:50.123  DEBUG # 3        GAME ( 97)  SOLO
(0x00057): election LOST 0xb0000000 (repl=b0000009/30000000)
+ SOLO (0x00057): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 250:  mm/dd/yy  11:48:50.131  DEBUG # 3        GAME ( 97)  SOLO
(0x00057): election CLOSED
0x10000000 (repl=b0000009/30000000)
```

The configuration file has a different link module than the one actually in the slot.

```
@ 273:  mm/dd/yy  11:48:51.240  WARN  # 3      LOADER (  6)  Link Module
on slot 3 misconfigured - ignoring
```

Slot 3 uses the dynamic loader to load the necessary executable modules from Slot 2's memory, not the memory card in Slot 2. But if a module is not in Slot 2's memory, the dynamic loader gets it from the router software image on the memory card.

```
@ 275:  mm/dd/yy  11:48:51.275  DEBUG # 2      LOADER ( 32)  Loader
serving request for ip.exe from 0x1000602a
+ Loader serving request for snmp.exe from 0x1000602b
@ 276:  mm/dd/yy  11:48:51.279  DEBUG # 3      LOADER ( 27)  Dynamic
loader transaction with slot 2 server for ip.exe:
+     start address 0x304E9770, size 0x00020984, checksum 0x00976221
```

```
@ 277:  mm/dd/yy  11:48:51.279  DEBUG # 2      LOADER ( 32) Loader
serving request for tftp.exe from 0x1000602c
@ 278:  mm/dd/yy  11:48:51.291  DEBUG # 3      LOADER ( 27) Dynamic
loader transaction with slot 2 server for snmp.exe:
+     start address 0x304A86E0, size 0x00007204, checksum 0x00211745
@ 279:  mm/dd/yy  11:48:51.295  DEBUG # 3      LOADER ( 27) Dynamic
loader transaction with slot 2 server for tftp.exe:
+     start address 0x304A2190, size 0x00003f54, checksum 0x00127cd1
@ 280:  mm/dd/yy  11:48:51.303  DEBUG # 2      LOADER ( 33) Loader
service completed for tftp.exe, 0x1000602c
@ 281:  mm/dd/yy  11:48:51.318  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for tftp.exe
@ 282:  mm/dd/yy  11:48:51.326  DEBUG # 3      LOADER ( 15) Loader
starting application tftp.exe, address 0x304e7f20, gate id = 0x0001c
@ 283:  mm/dd/yy  11:48:51.326  DEBUG # 2      LOADER ( 33) Loader
service completed for snmp.exe, 0x1000602b
@ 284:  mm/dd/yy  11:48:51.330  INFO  # 3        TFTP (  2) Protocol
initializing.
@ 285:  mm/dd/yy  11:48:51.330  DEBUG # 3        TFTP ( 15) Subsystem
transitioned to DOWN state.
@ 286:  mm/dd/yy  11:48:51.357  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for snmp.exe
@ 287:  mm/dd/yy  11:48:51.365  DEBUG # 3      LOADER ( 15) Loader
starting application snmp.exe, address 0x304ebe90, gate id = 0x00019
@ 288:  mm/dd/yy  11:48:51.377  INFO  # 3        SNMP (  7) Protocol
initializing.
@ 289:  mm/dd/yy  11:48:51.408  DEBUG # 3        SNMP ( 36) Agent received
new community public, assigned index 1.
@ 290:  mm/dd/yy  11:48:51.432  DEBUG # 3        SNMP ( 38) Agent received
new manager 0 for community index 1
@ 291:  mm/dd/yy  11:48:51.475  DEBUG # 2      LOADER ( 33) Loader
service completed for ip.exe, 0x1000602a
@ 298:  mm/dd/yy  11:48:51.572  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for ip.exe
@ 299:  mm/dd/yy  11:48:51.600  DEBUG # 3      LOADER ( 15) Loader
starting application ip.exe, address 0x304f30b0, gate id = 0x00048
```

The IP RTM updates its bit map to indicate it is running on Slot 3.

```
@ 300:  mm/dd/yy  11:48:51.623  INFO  # 3          IP (  4) Protocol
initializing
@ 301:  mm/dd/yy  11:48:51.631  DEBUG # 2          IP (  8) RTM self map
old a0000049,  new b0000049
```

Slot 3 reads the driver needed for a SYNC port from *bn.exe*.

```
@ 309:  mm/dd/yy  11:48:52.080  DEBUG # 2        NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
```

```
@ 310:  mm/dd/yy  11:48:52.564  DEBUG # 3      LOADER ( 30)  Image
hdlc.exe loaded successfully from 2:bn.exe
@ 311:  mm/dd/yy  11:48:52.564  DEBUG # 2        NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 312:  mm/dd/yy  11:48:52.584  DEBUG # 3      LOADER ( 15)  Loader
starting application hdlc.exe, address 0x304d2130, gate id = 0x00041
@ 313:  mm/dd/yy  11:48:52.588  INFO  # 3        SYNC (  7)  Service
initializing.
```

AppleTalk (entity AT) successfully loads and initializes on Slot 3. The operating system elects to run the AppleTalk MIB soloist on slot 3, and AppleTalk updates the AT RTM bit map accordingly.

```
@ 314:  mm/dd/yy  11:48:52.689  DEBUG # 2        NVFS ( 63)  NVFS manager
is opening file 'bn.exe' for reading
@ 316:  mm/dd/yy  11:48:53.229  DEBUG # 3      LOADER ( 30)  Image at.exe
loaded successfully from 2:bn.exe
@ 321:  mm/dd/yy  11:48:53.256  DEBUG # 3      LOADER ( 15)  Loader
starting application at.exe, address 0x304bc3c0, gate id = 0x00071
@ 322:  mm/dd/yy  11:48:53.260  DEBUG # 2        TFTP ( 16)  Subsystem
transitioned to READY state.
+ Client initialized.
@ 323:  mm/dd/yy  11:48:53.283  INFO  # 3  APPLETALK (  4)  Protocol
initializing
@ 324:  mm/dd/yy  11:48:53.369  DEBUG # 3        GAME ( 23)  SOLO
(0x000a5): election opening 30000000/30000000 (30000000) vote=00000000
@ 325:  mm/dd/yy  11:48:53.381  DEBUG # 3        GAME ( 97)  SOLO
(0x000a5): election WON 0x10000000 (repl=b0000009/30000000)
+ SOLO (0x000a5): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 326:  mm/dd/yy  11:48:53.396  DEBUG # 3        GAME ( 97)  SOLO
(0x000a5): election CLOSED 0x10000000 (repl=b0000009/30000000)
@ 327:  mm/dd/yy  11:48:53.404  DEBUG # 3  APPLETALK ( 43)
at_rtm_self_map: old 00000072 new 90000072
@ 328:  mm/dd/yy  11:48:53.416  DEBUG # 3  APPLETALK ( 43)
at_mib_solo_chg: BECAME_LOCAL old 000000a5 new 900000a5
+ at_rtm_self_chg: old 00000072 new 90000072
```

The following log messages show what happens when you use the Configuration Manager in dynamic mode to create TCP and Telnet. The subsequent lines show that the MIB entity modifies the MIB objects for TCP and Telnet, thereby causing these applications to initialize.

```
@ 343:  mm/dd/yy  11:50:29.005  INFO  # 2         MIB (  7)  wfSnmp.3.0 set
to 128.128.2.3
@ 344:  mm/dd/yy  11:50:29.096  INFO  # 2         MIB (  5)  wfTcp.2.0 set
to 1
```

```
@ 345:  mm/dd/yy  11:50:29.741  INFO  # 2        MIB ( 9)  wfNode.2.0 set
to 0x51e3200000000000
@ 346:  mm/dd/yy  11:50:45.598  INFO  # 2        MIB ( 5)  wfTelnet.2.0
set to 1
@ 347:  mm/dd/yy  11:50:45.839  INFO  # 2        MIB ( 9)  wfNode.2.0 set
to 0x51e3200400000000
```

The object wfProtocols is the protocol bit-map object. Each attribute is a different protocol. Every time you add or delete a protocol from a slot, the MIB entity updates the bit map for that protocol. Do *not* try to use the Technician Interface to update this field.

```
@ 348:  mm/dd/yy  11:50:46.188  INFO  # 2        MIB ( 6)
wfProtocols.18.0 set to 1610612736
@ 349:  mm/dd/yy  11:50:46.420  INFO  # 2        MIB ( 6)
wfProtocols.15.0 set to 1610612736
```

NVFS reads the Telnet and TCP executable modules from memory card in Slot 2; the dynamic loader loads them in Slot 2.

```
@ 350:  mm/dd/yy  11:50:46.762  DEBUG # 2        NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 351:  mm/dd/yy  11:50:46.932  DEBUG # 3        LOADER ( 27) Dynamic
loader transaction with slot 2 server for tcp.exe:
+    start address 0x304797B0, size 0x0000cec4, checksum 0x00394408
@ 352:  mm/dd/yy  11:50:47.015  DEBUG # 3        LOADER ( 28) Dynamic
loader completed transaction for tcp.exe
@ 353:  mm/dd/yy  11:50:47.032  DEBUG # 3        LOADER ( 15) Loader
starting application tcp.exe, address 0x304ad4d0, gate id = 0x0007b
@ 354:  mm/dd/yy  11:50:47.061  INFO  # 3        TCP ( 5)  TCP is UP.
@ 355:  mm/dd/yy  11:50:47.086  DEBUG # 2     LOADER ( 30)  Image tcp.exe
loaded successfully from 2:bn.exe
@ 356:  mm/dd/yy  11:50:47.086  DEBUG # 2        NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 357:  mm/dd/yy  11:50:47.107  DEBUG # 2     LOADER ( 15)  Loader
starting application tcp.exe, address 0x304797b0, gate id = 0x0007b
@ 358:  mm/dd/yy  11:50:47.123  DEBUG # 2     LOADER ( 32)  Loader
serving request for tcp.exe from 0x10006057
@ 359:  mm/dd/yy  11:50:47.139  INFO  # 2        TCP ( 5)  TCP is UP.
@ 360:  mm/dd/yy  11:50:47.180  DEBUG # 2     LOADER ( 33)  Loader
service completed for tcp.exe, 0x10006057
@ 361:  mm/dd/yy  11:50:47.259  DEBUG # 2        NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 362:  mm/dd/yy  11:50:47.553  DEBUG # 3     LOADER ( 30)  Image tn.exe
loaded successfully from 2:bn.exe
@ 363:  mm/dd/yy  11:50:47.569  DEBUG # 3        LOADER ( 15) Loader
starting application tn.exe, address 0x304a3cb0, gate id = 0x00076
+ Loader serving request for tn.exe from 0x200040df
```

```
@ 364:  mm/dd/yy  11:50:47.569  INFO  # 3     TELNET (  4)  Connection
Manager initializing.
@ 365:  mm/dd/yy  11:50:47.598  DEBUG # 3       TCP ( 14)  TCP Open req:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x30530670
@ 366:  mm/dd/yy  11:50:47.639  DEBUG # 3     LOADER ( 33)  Loader
service completed for tn.exe, 0x200040df
@ 367:  mm/dd/yy  11:50:47.660  INFO  # 3       TCP (  6)  TCP Opened:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x30530670
@ 368:  mm/dd/yy  11:50:47.660  INFO  # 3     TELNET (  5)  Connection
Manager listening on TCP port 23
@ 369:  mm/dd/yy  11:50:47.745  DEBUG # 2       NVFS ( 64)  NVFS manager
is closing file 'bn.exe'
@ 370:  mm/dd/yy  11:50:47.766  DEBUG # 2     LOADER ( 27)  Dynamic
loader transaction with slot 3 server for tn.exe:
+     start address 0x304A3CB0, size 0x00009808, checksum 0x002bb03b
@ 371:  mm/dd/yy  11:50:47.853  DEBUG # 2     LOADER ( 28)  Dynamic
loader completed transaction for tn.exe
@ 372:  mm/dd/yy  11:50:47.866  DEBUG # 2     LOADER ( 15)  Loader
starting application tn.exe, address 0x3046ff90, gate id = 0x00076
@ 373:  mm/dd/yy  11:50:47.866  INFO  # 2     TELNET (  4)  Connection
Manager initializing.
@ 374:  mm/dd/yy  11:50:47.886  DEBUG # 2       TCP ( 14)  TCP Open req:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x304e6830
@ 375:  mm/dd/yy  11:50:47.923  DEBUG # 2        IP ( 36)  Client on
128.128.2.2 for TCP local 23 remote 0 is up
@ 376:  mm/dd/yy  11:50:47.943  INFO  # 2       TCP (  6)  TCP Opened:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x304e6830
@ 377:  mm/dd/yy  11:50:47.943  INFO  # 2     TELNET (  5)  Connection
Manager listening on TCP port 23
@ 378:  mm/dd/yy  11:50:49.031  DEBUG # 2        IP ( 36)  Client on
128.128.2.2 for TCP local 23 remote 0 is up
```

The following log messages show what happens when you remove the link
module in Slot 3: Data Path kills the gate assigned to the circuit that becomes
unavailable.

```
@ 383:  mm/dd/yy  11:51:10.612  WARN  # 2     MODULE (  3)  I/O module has
been removed.
@ 386:  mm/dd/yy  11:51:10.632  DEBUG # 2        DP ( 23)  dp_line_map -
Line GH 0xa0004082 died, cct 1
@ 387:  mm/dd/yy  11:51:10.640  DEBUG # 2        DP ( 41)  LINE_DOWN msg
rcvd for line gate 0x20004082 on cct 1.
+ Found dead line 0x20004082 at offset 0
+ Last line 0x20004082 in cct 1 died, killing circuit gate
+ DP killing CC gate for cct 1.
```

In this example, the user issued a command to save a log file to the memory card:

```
@ 403:  mm/dd/yy  11:52:07.684  DEBUG # 2      NVFS ( 63)  NVFS manager
is opening file 'log.sav' for writing
```

Dial-on-Demand Raise DTR Log

The following log shows a successful dial-on-demand connection between the COM2 port in Slot 2 and a modem configured for Raise DTR.

These messages appear only when you click on the port configured for dial-on-demand, and set the Debug option under the Modem definition to Enabled. If you are using the Technician Interface, set attribute #29 (the debug attribute) of the object wfModemIfEntry to 1 (1 = enabled, 2 = disabled).   The Debug option is available with Software Version 8.01 and later.

The following message indicates that the Sync software module enabled the COM2 port.

```
#    33: mm/dd/yy 14:14:02.826  INFO       SLOT  2  SYNC    Code:    9
Connector COM2 enabled.
```

The port completes initialization.

```
#    34: mm/dd/yy 14:14:03.095  DEBUG      SLOT  2  SYNC    Code:   16
Connector COM2 initialization complete
    Environment address      - 3051f040 Line record address      - 3052d8bc
    Hardware map address     - 30514f9c Initialization block     -
80007800
    Receive descriptor ring - 80005000 Transmit descriptor ring -
80005800
#    35: mm/dd/yy 14:14:03.095  DEBUG      SLOT  2  PCAP    Code:   67
interface became local - line 202102
intf gate spawned - line 202102
#    36: mm/dd/yy 14:14:03.103  DEBUG      SLOT  2  PCAP    Code:   65
wait_state - line 202102
```

The FSM (finite state machine) messages indicate that communication between the modem and the router is occurring. The first FSM message shows the state the router is currently in when the "FSM Event" that follows occurred.

```
#    37: mm/dd/yy 14:14:04.100  DEBUG      SLOT  2  SWSERV    Code:   46
Connector COM2: FSM State: RDTR_DISCONNECTED(0)
Connector COM2: FSM Event: RDTR_EVENT_CCT_UP(1); isdn flags: 0x0
```

The following messages indicate that you configured the port for Raise DTR, rather than V.25bis, and remind you to check the modem connection.

```
#    38: mm/dd/yy 14:14:04.100  INFO       SLOT  2  MODEMIF   Code:   22
Connector COM2: enable requested on cct 65535
Connector COM2: Starting, raise dtr mode, is modem connected and turned
on?
```

The following messages appear even if you did not connect a modem to the router. Unlike V.25bis, Raise DTR does not look for a pin signal to detect whether the port is attached to a modem.

```
#    39: mm/dd/yy 14:14:04.104  INFO      SLOT  2  MODEMIF   Code:  52
Connector COM2: Circuit has been brought up.
#    40: mm/dd/yy 14:14:04.104  DEBUG     SLOT  2  SWSERV    Code:  46
Line Mgr received line ready for line 2
#    41: mm/dd/yy 14:14:04.104  INFO      SLOT  2  SWSERV    Code:  10
Sync Line 2 available for dial on demand pool 2.
#    42: mm/dd/yy 14:14:04.108  INFO      SLOT  2  SYNC   Code:  11
Connector COM2 providing LLC1 service.
#    43: mm/dd/yy 14:14:04.636  DEBUG     SLOT  2  SWSERV    Code:  46
Connector COM2: FSM State: RDTR_WAIT_DATA_OR_IND(1)
Connector COM2: FSM Event: RDTR_EVENT_CD_UP(6); isdn flags: 0x24
#    44: mm/dd/yy 14:15:07.770  INFO      SLOT  2  SWSERV    Code:  23
Data received for dial on demand circuit 3.
```

The log messages stop here until you connect and turn on a modem. After you do this, the router raises DTR to signal the local modem to dial the phone number of the remote modem. The router then pings the remote side of the dial-on-demand link, and displays a "data available" message when it receives a response.

```
#    45: mm/dd/yy 14:15:07.774  DEBUG     SLOT  2  SWSERV    Code:  46
Connector COM2: FSM State: RDTR_WAIT_DATA_OR_IND(1)
Connector COM2: FSM Event: RDTR_EVENT_DATA_AVAIL(5); isdn flags: 0x2c
#    46: mm/dd/yy 14:15:07.774  TRACE     SLOT  2  MODEMIF   Code:  34
Connector COM2: DATA Available.
```

The software assigns a valid circuit number to the line.

```
#    47: mm/dd/yy 14:15:07.774  DEBUG     SLOT  2  SWSERV    Code:  44
SW Sent you are cc 3 message to line 2
#    48: mm/dd/yy 14:15:07.782  INFO      SLOT  2  SWSERV    Code:   7
Dial on demand circuit being established on line 2.
```

The router waits for DSR to come up to indicate the modem established connection to the remote node.

```
#    49: mm/dd/yy 14:15:32.552  DEBUG     SLOT  2  SWSERV    Code:  46
Connector COM2: FSM State: RDTR_WAIT_FOR_DSR(2)
Connector COM2: FSM Event: RDTR_EVENT_DSR_UP(3); isdn flags: 0x2e
```

DSR is up.

```
#    50: mm/dd/yy 14:15:32.552  TRACE     SLOT  2  MODEMIF   Code:  54
Connector COM2: DSR has come up.
#    51: mm/dd/yy 14:15:32.552  INFO      SLOT  2  MODEMIF   Code:  31
Connector COM2: Connection established.
```

The PPP link over the dial-on-demand circuit establishes an LCP (Link Control Protocol) connection. The messages beginning with Message 57 show that the network protocol (IP) software starts and that IP establishes a connection over the dial-on-demand link.

```
#    52: mm/dd/yy 14:15:32.552  TRACE    SLOT  2  PPP    Code:   43
Sending LCP Configure-Request on circuit 3.
#    53: mm/dd/yy 14:15:32.681  TRACE    SLOT  2  PPP    Code:   55
Received LCP Configure-Ack on circuit 3.
#    54: mm/dd/yy 14:15:34.867  TRACE    SLOT  2  PPP    Code:   43
Sending LCP Configure-Request on circuit 3.
#    55: mm/dd/yy 14:15:34.875  TRACE    SLOT  2  PPP    Code:   54
Received LCP Configure-Request on circuit 3.
Sending LCP Configure-Ack on circuit 3.
#    56: mm/dd/yy 14:15:34.992  TRACE    SLOT  2  PPP    Code:   55
Received LCP Configure-Ack on circuit 3.
#    57: mm/dd/yy 14:15:34.992  INFO     SLOT  2  PPP    Code:   38
Link Establishment Phase complete on circuit 3.
Starting Network Control Protocols on circuit 3.
#    58: mm/dd/yy 14:15:34.992  TRACE    SLOT  2  PPP    Code:   43
Sending IPCP Configure-Request on circuit 3.
#    59: mm/dd/yy 14:15:34.996  INFO     SLOT  2  PPP    Code:   28
LCP up on circuit 3.
#    60: mm/dd/yy 14:15:35.003  TRACE    SLOT  2  PPP    Code:   54
Received IPCP Configure-Request on circuit 3.
#    61: mm/dd/yy 14:15:35.007  TRACE    SLOT  2  PPP    Code:   63
IPCP Naking IP-Address option value 0x0 with value 0x3030301 on circuit
3.
Sending IPCP Configure-Nak on circuit 3.
#    66: mm/dd/yy 14:15:35.117  TRACE    SLOT  2  PPP    Code:   55
Received IPCP Configure-Ack on circuit 3.
#    67: mm/dd/yy 14:15:35.128  TRACE    SLOT  2  PPP    Code:   54
Received IPCP Configure-Request on circuit 3.
#    68: mm/dd/yy 14:15:35.132  TRACE    SLOT  2  PPP    Code:   44
Sending IPCP Configure-Ack on circuit 3.
#    69: mm/dd/yy 14:15:35.132  INFO     SLOT  2  PPP    Code:   28
IPCP up on circuit 3.
```

The following messages indicate that the Raise DTR signal causes the software to establish the link and activate the upper-layer protocol. ULI stands for Upper Layer Indicator.

```
#    70: mm/dd/yy 14:15:35.136  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM2: FSM State: RDTR_WAIT_FOR_ULI(3)
Connector COM2: FSM Event: RDTR_EVENT_ULI_IND(8); isdn flags: 0x22e
#    71: mm/dd/yy 14:15:56.980  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM2: FSM State: RDTR_CONNECTED(4)
Connector COM2: FSM Event: RDTR_EVENT_DSR_DN(4); isdn flags: 0x224
```

The router detected that the modem dropped DSR, indicating the remote link is lost.

```
#    72: mm/dd/yy 14:15:56.980  TRACE    SLOT  2  MODEMIF   Code:  32
Connector COM2: DSR lost connection closed.
```

The router exceeds its inactivity timeout threshold, and drops DTR to terminate the connection to the modem.

```
#    73: mm/dd/yy 14:15:56.980  DEBUG    SLOT  2  SWSERV    Code:  46
isdn_down_cct - calling drop_dtr
```

The router disables PPP.

```
#    74: mm/dd/yy 14:15:56.980  INFO     SLOT  2  PPP     Code:  31
Stopping Network Control Protocols on circuit 3.
IPCP down on circuit 3.
LCP down on circuit 3.
#    75: mm/dd/yy 14:15:57.035  INFO     SLOT  2  SYNC    Code:  13
Connector COM2 LLC1 service withdrawn.
```

The following message is normal after a dial-on-demand connection terminates.

```
#    76: mm/dd/yy 14:15:57.039  DEBUG    SLOT  2  SWSERV    Code:  46
Demand line failed for circuit 3.
sw_dd_line_fail set in use circuit to zero for com 2.
```

The router completes the orderly termination of the dial-on-demand link by re-initializing the port.

```
#    77: mm/dd/yy 14:15:57.054  INFO     SLOT  2  SYNC    Code:   9
Connector COM2 enabled.
#    78: mm/dd/yy 14:15:57.364  DEBUG    SLOT  2  SYNC    Code:  16
Connector COM2 initialization complete
    Environment address    - 3051f040 Line record address     - 3052d8bc
    Hardware map address    - 30514f9c Initialization block    -
80007800
    Receive descriptor ring - 80005000 Transmit descriptor ring -
80005800
#    79: mm/dd/yy 14:15:57.364  DEBUG    SLOT  2  PCAP    Code:  67
interface became local - line 202102
#    80: mm/dd/yy 14:15:57.368  DEBUG    SLOT  2  PCAP    Code:  68
```

```
intf gate spawned - line 202102
```

The router returns to a "wait_state," a state in which it is waiting for data.

```
#    81: mm/dd/yy 14:15:57.372  DEBUG    SLOT  2  PCAP    Code:  65
wait_state - line 202102
#    82: mm/dd/yy 14:15:58.401  DEBUG    SLOT  2  SWSERV   Code:  46
Connector COM2: FSM State: RDTR_DISCONNECTED(0)
Connector COM2: FSM Event: RDTR_EVENT_CCT_UP(1); isdn flags: 0x0
#    83: mm/dd/yy 14:15:58.401  INFO     SLOT  2  MODEMIF  Code:  22
Connector COM2: enable requested on cct 65535
Connector COM2: Starting, raise dtr mode, is modem connected and turned
on?
Connector COM2: Circuit has been brought up.
```

Dial-on-Demand V.25bis

The following log shows a successful dial-on-demand connection between the
COM1 port in Slot 2 and a modem configured for V.25bis.

These messages appear only when you click on the port configured for
dial-on-demand, and set the Debug option under the Modem definition to
Enabled. If you are using the Technician Interface, set attribute #29 (the debug
attribute) of the object wfModemIfEntry to 1 (1 = enabled, 2 = disabled).   The
Debug option is available with Software Version 8.01 and later.

The following message indicates that the Sync software module enabled the
COM1 port.

```
#     9: mm/dd/yy 13:07:24.725  INFO     SLOT  2  SYNC    Code:   9
Connector COM1 enabled.
```

The port completes initialization.

```
#    10: mm/dd/yy 13:07:24.995  DEBUG    SLOT  2  SYNC    Code:  16
Connector COM1 initialization complete
    Environment address    - 3051ea30 Line record address    - 3052e03c
    Hardware map address    - 30526e3c Initialization block    -
80007c00
    Receive descriptor ring - 80006000 Transmit descriptor ring -
80006800
#    11: mm/dd/yy 13:07:24.995  DEBUG    SLOT  2  PCAP    Code:  67
interface became local - line 202101
intf gate spawned - line 202101
```

```
#    12: mm/dd/yy 13:07:25.002  DEBUG     SLOT  2  PCAP     Code:  65
wait_state - line 202101
```

The FSM (finite state machine) messages indicate that communication between the modem and the router is occurring. The first FSM message shows the state the router is currently in when the "FSM Event" that follows occurred.

```
#    13: mm/dd/yy 13:07:26.031  DEBUG     SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_DISCONNECTED(0)
Connector COM1: FSM Event: V25BIS_EVENT_CCT_UP(1); isdn flags: 0x0
```

The port uses the CTS (clear to send) pin signal to determine whether a modem is present.

```
#    14: mm/dd/yy 13:07:26.031  INFO      SLOT  2  MODEMIF   Code:  22
Connector COM1: enable requested on cct 65535
```

The circuit number 65535 does not activate until data is waiting to transmit across the connection.

The FSM (Finite State Machine) messages indicate that communication between the modem and the router is occurring. The first FSM message shows the state the router is currently in when the "FSM Event" that follows occurred.

```
#    15: mm/dd/yy 13:07:26.591  DEBUG     SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_CTS(1)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x1
#    16: mm/dd/yy 13:07:26.591  TRACE     SLOT  2  MODEMIF   Code:  53
Connector COM1: CTS has come up.
```

The router believes a V.25bis modem is present because it detected a CTS signal. The following message indicates that you configured the port for V.25bis, rather than Raise DTR.

```
#    17: mm/dd/yy 13:07:26.591  DEBUG     SLOT  2  MODEMIF   Code:   9
Connector COM1: modem present V.25bis mode
#    18: mm/dd/yy 13:07:26.591  DEBUG     SLOT  2  SWSERV    Code:  46
Line Mgr received line ready for line 1
#    19: mm/dd/yy 13:07:26.591  INFO      SLOT  2  SWSERV    Code:  10
Sync Line 1 available for dial on demand pool 1.
```

The router provides LLC service on the dial-on-demand port only after it detects a CTS signal.

```
#    20: mm/dd/yy 13:07:26.591  INFO      SLOT  2  SYNC     Code:  11
Connector COM1 providing LLC1 service.
```

The router pings the remote side of the dial-on-demand link to provide data to transmit across the link, and displays a "data received" message when it receives a response.

```
#    21: mm/dd/yy 13:09:16.174  INFO     SLOT  2  SWSERV    Code:  23
Data received for dial on demand circuit 2.
#    22: mm/dd/yy 13:09:16.178  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_WAIT_DATA_OR_IND(2)
Connector COM1: FSM Event: V25BIS_EVENT_DATA_AVAIL(7); isdn flags: 0x9
#    23: mm/dd/yy 13:09:16.178  TRACE    SLOT  2  MODEMIF   Code:  34
Connector COM1: DATA Available.
#    24: mm/dd/yy 13:09:16.178  DEBUG    SLOT  2  SWSERV    Code:  44
SW Sent you are cc 2 message to line 1
The line is given a valid circuit number (2) in order to be activated
#    25: mm/dd/yy 13:09:16.193  INFO     SLOT  2  SWSERV    Code:   7
Dial on demand circuit being established on line 1.
```

The router forwards a call request number (CRN) to the V.25bis modem. It uses the phone number configured in the "Outgoing" field of the circuit definition.

```
#    26: mm/dd/yy 13:09:16.225  TRACE    SLOT  2  MODEMIF   Code:  35
Connector COM1: Sent CRN cmd to T3053
```

In this example, the cable connection to the modem is loose. The router fails to receive a response from the modem indicating that it received the CRN. The router exceeds its inactivity timeout threshold, and drops DTR to terminate the connection to the modem.

```
#    27: mm/dd/yy 13:10:17.446  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ADAP_RSP(3)
Connector COM1: FSM Event: V25BIS_EVENT_TO(0); isdn flags: 0x4009
isdn_fsm_TO_WAIT - calling drop_dtr
#    28: mm/dd/yy 13:10:18.518  TRACE    SLOT  2  MODEMIF   Code:  27
Connector COM1: Connection timeout, retry in progress
#    29: mm/dd/yy 13:10:18.518  DEBUG    SLOT  2  SWSERV    Code:  46
Before g_delay for retry timer in - isdn_fsm_CONN_DELAY_IND
```

The router reinitializes the link with the modem after detecting CTS is high.

```
#    30: mm/dd/yy 13:10:18.784  TRACE    SLOT  2  MODEMIF   Code:  53
Connector COM1: CTS has come up.
#    31: mm/dd/yy 13:10:18.784  DEBUG    SLOT  2  MODEMIF   Code:   9
Connector COM1: modem present V.25bis mode
```

Once again, the router sends the CRN to the modem.

```
#    32: mm/dd/yy 13:10:18.784  TRACE    SLOT  2  MODEMIF    Code:  35
Connector COM1: Sent CRN cmd to T3053
#    65: mm/dd/yy 13:12:58.985  TRACE    SLOT  2  MODEMIF    Code:  35
Connector COM1: Sent CRN cmd to T3053
#    66: mm/dd/yy 13:12:59.032  DEBUG    SLOT  2  SWSERV     Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ADAP_RSP(3)
Connector COM1: FSM Event: V25BIS_EVENT_VALID_RSP(8); isdn flags: 0x4009
```

The messages assume that you reconnected the cable to the modem.

The router receives a response from the modem.

```
#    67: mm/dd/yy 13:12:59.032  TRACE    SLOT  2  MODEMIF    Code:  38
Connector COM1: Adapter accepted CRN command
```

The router now waits for the modem to raise DSR. It detects that the modem dropped CTS. The modem does this to prevent the router from sending more data to it until it establishes a connection with the remote modem.

```
#    68: mm/dd/yy 13:13:02.075  DEBUG    SLOT  2  SWSERV     Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_DN(6); isdn flags: 0x4008
#    69: mm/dd/yy 13:13:23.263  DEBUG    SLOT  2  SWSERV     Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
```

The router receives a signal from the modem indicating that the connection between the modems is up.

```
#    70: mm/dd/yy 13:13:23.267  DEBUG    SLOT  2  SWSERV     Code:  46
Connector COM1: FSM Event: V25BIS_EVENT_CONN_IND(11); isdn flags: 0x4008
#    71: mm/dd/yy 13:13:23.267  INFO     SLOT  2  MODEMIF    Code:  46
Connector COM1: Received a connect indication (CNX)
```

The modem raises DSR and CTS.

```
#    72: mm/dd/yy 13:13:23.673  DEBUG    SLOT  2  SWSERV     Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x4009
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_DSR_UP(3); isdn flags: 0x400b
```

The router determines that a successful connection is available between both routers connected via the dial-on-demand link.

```
#    73: mm/dd/yy 13:13:23.673  TRACE    SLOT  2  MODEMIF    Code:  54
Connector COM1: DSR has come up.
#    74: mm/dd/yy 13:13:23.673  INFO     SLOT  2  MODEMIF    Code:  31
Connector COM1: Connection established.
#    75: mm/dd/yy 13:13:23.677  TRACE    SLOT  2  PPP     Code:  43
```

```
Sending LCP Configure-Request on circuit 2.
#    76: mm/dd/yy 13:13:23.806  TRACE    SLOT  2  PPP     Code:  55
Received LCP Configure-Ack on circuit 2.
#    77: mm/dd/yy 13:13:25.930  TRACE    SLOT  2  PPP     Code:  54
Received LCP Configure-Request on circuit 2.
Sending LCP Configure-Ack on circuit 2.
#    78: mm/dd/yy 13:13:25.930  INFO     SLOT  2  PPP     Code:  38
Link Establishment Phase complete on circuit 2.
Starting Network Control Protocols on circuit 2.
```

The PPP link over the dial-on-demand circuit establishes an LCP (Link Control Protocol) connection. The IP software starts and IP establishes a connection over the dial-on-demand link.

```
#    79: mm/dd/yy 13:13:25.930  TRACE    SLOT  2  PPP     Code:  43
Sending IPCP Configure-Request on circuit 2.
#    80: mm/dd/yy 13:13:25.930  INFO     SLOT  2  PPP     Code:  28
LCP up on circuit 2.
#    81: mm/dd/yy 13:13:26.058  TRACE    SLOT  2  PPP     Code:  54
Received IPCP Configure-Request on circuit 2.
IPCP Naking IP-Address option value 0x0 with value 0x2020201 on circuit
2.
Sending IPCP Configure-Nak on circuit 2.
#    84: mm/dd/yy 13:13:26.094  TRACE    SLOT  2  PPP     Code:  55
Received IPCP Configure-Ack on circuit 2.
#    85: mm/dd/yy 13:13:26.220  TRACE    SLOT  2  PPP     Code:  54
Received IPCP Configure-Request on circuit 2.
#    86: mm/dd/yy 13:13:26.224  TRACE    SLOT  2  PPP     Code:  44
Sending IPCP Configure-Ack on circuit 2.
#    87: mm/dd/yy 13:13:26.224  INFO     SLOT  2  PPP     Code:  28
IPCP up on circuit 2.
```

The protocol on top of the dial-on-demand link is active. The V.25bis communication ends. The modem dropped the DSR signal to the router, and the router in turn dropped DTR to terminate the connection to the modem. ULI stands for upper layer indication.

```
#    88: mm/dd/yy 13:13:26.224  DEBUG    SLOT  2  SWSERV   Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ULI(6)
```

```
#    89: mm/dd/yy 13:13:26.228  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM Event: V25BIS_EVENT_ULI_IND(15); isdn flags: 0x420b
#    90: mm/dd/yy 13:13:51.529  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_CONNECTED(7)
Connector COM1: FSM Event: V25BIS_EVENT_DSR_DN(4); isdn flags: 0x4201
#    91: mm/dd/yy 13:13:51.529  TRACE    SLOT  2  MODEMIF   Code:  32
Connector COM1: DSR lost connection closed.
#    92: mm/dd/yy 13:13:51.529  DEBUG    SLOT  2  SWSERV    Code:  46
isdn_down_cct - calling drop_dtr
#    93: mm/dd/yy 13:13:51.529  INFO     SLOT  2  PPP       Code:  31
Stopping Network Control Protocols on circuit 2.
IPCP down on circuit 2.
LCP down on circuit 2.
#    94: mm/dd/yy 13:13:51.552  INFO     SLOT  2  SYNC      Code:  13
Connector COM1 LLC1 service withdrawn.
```

The following message is normal after a dial-on-demand connection terminates.

```
#    95: mm/dd/yy 13:13:51.556  DEBUG    SLOT  2  SWSERV    Code:  46
Demand line failed for circuit 2.
sw_dd_line_fail set in use circuit to zero for com 1.
```

The router completes the orderly termination of the dial-on-demand link by re-initializing the port.

```
#    96: mm/dd/yy 13:13:51.572  INFO     SLOT  2  SYNC      Code:   9
Connector COM1 enabled.
#    97: mm/dd/yy 13:13:51.841  DEBUG    SLOT  2  SYNC      Code:  16
Connector COM1 initialization complete
    Environment address     - 3051ea30 Line record address     - 3052e03c
    Hardware map address    - 30526e3c Initialization block     -
80007c00
    Receive descriptor ring - 80006000 Transmit descriptor ring -
80006800
#    98: mm/dd/yy 13:13:51.841  DEBUG    SLOT  2  PCAP      Code:  67
interface became local - line 202101
intf gate spawned - line 202101
#    99: mm/dd/yy 13:13:51.849  DEBUG    SLOT  2  PCAP      Code:  65
wait_state - line 202101
#   100: mm/dd/yy 13:13:52.846  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_DISCONNECTED(0)
Connector COM1: FSM Event: V25BIS_EVENT_CCT_UP(1); isdn flags: 0x0
#   101: mm/dd/yy 13:13:52.846  INFO     SLOT  2  MODEMIF   Code:  22
Connector COM1: enable requested on cct 65535
#   102: mm/dd/yy 13:13:53.406  DEBUG    SLOT  2  SWSERV    Code:  46
Connector COM1: FSM State: V25BIS_WAIT_FOR_CTS(1)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x1
#   103: mm/dd/yy 13:13:53.406  TRACE    SLOT  2  MODEMIF   Code:  53
Connector COM1: CTS has come up.
```

```
#   104: mm/dd/yy 13:13:53.406  DEBUG    SLOT  2  MODEMIF    Code:    9
Connector COM1: modem present V.25bis mode
#   105: mm/dd/yy 13:13:53.406  DEBUG    SLOT  2  SWSERV     Code:   46
Line Mgr received line ready for line 1
#   106: mm/dd/yy 13:13:53.406  INFO     SLOT  2  SWSERV     Code:   10
Sync Line 1 available for dial on demand pool 1.
#   107: mm/dd/yy 13:13:53.406  INFO     SLOT  2  SYNC   Code:   11
Connector COM1 providing LLC1 service.
```

MCT1 Log Information in a Lab Testing Environment

The following log messages show what happens when you access the Line Tests option and use Port 2 of an MCT1-2 in Slot 5 to send a payload loopback to Port 1 of an MCT1-2 Slot 4. During this test, the yellow loopback LED lights on Port 1 in Slot 4.

When you enter the Technician Interface script command **show ds1e1 port**, the Technician Interface accesses the *MCT1.bat* file and the MIB, and displays the MCT1-2 port setup.

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Payload	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

When the remote slot (Slot 4) receives a loop-up or loop-down command, the remote loopback yellow LED lights and the following messages appear in the log:

```
#     2: mm/dd/yy 08:56:17.563   INFO      SLOT  4  DS1E1    Code:   55
Connector COM2 received loop-up code
#    18: mm/dd/yy 09:08:47.872   INFO      SLOT  4  DS1E1    Code:   56
Connector COM2 received loop-down code
#     3: mm/dd/yy 10:31:12.638   INFO      SLOT  2  MIB      Code:    5
wfDs1E1ActionEntry.5.905102 set to 5
#     4: mm/dd/yy 10:31:12.683   INFO      SLOT  4  DS1E1    Code:   30
Connector COM1 Unscheduled FDL message received - type Payload Loopback
Activate.
#     5: mm/dd/yy 10:31:12.687   INFO      SLOT  4  DS1E1    Code:   22
```

```
Connector COM1, Logical Line 1 LLC service withdrawn.
#    6: mm/dd/yy 10:31:33.105   WARNING   SLOT  5  DS1E1    Code:   4
Connector COM2, Logical Line 1 receiver timeout.
#    7: mm/dd/yy 10:31:33.109   DEBUG     SLOT  5  DP       Code:  23
dp_line_map - Line GH 0x8400b4e3 died, cct 3
#    8: mm/dd/yy 10:31:33.113   INFO      SLOT  5  DS1E1    Code:  22
Connector COM2, Logical Line 1 LLC service withdrawn.
#    9: mm/dd/yy 10:31:33.113   DEBUG     SLOT  5  DP       Code:  41
LINE_DOWN msg rcvd for line gate 0x400b4e3 on cct 3.
Found dead line 0x400b4e3 at offset 0
Last line 0x400b4e3 in cct 3 died, killing circuit gate
DP killing CC gate for cct 3.
#   10: mm/dd/yy 10:31:33.124   INFO      SLOT  5  IP       Code:   3
Interface 4.1.2.1 down on circuit 3
#   11: mm/dd/yy 10:31:33.148   INFO      SLOT  5  DP       Code:   2
Circuit 3 down.
#   14: mm/dd/yy 10:31:33.164   DEBUG     SLOT  5  GAME     Code:  84
FWD [ 5-60f0] (84000053->bc000403): down=3c000000, no_ACK=00000000,
NAK=3c000000
#   15: mm/dd/yy 10:31:33.230   DEBUG     SLOT  5  DS1E1    Code:  50
Connector COM2, Logical Line 1 time_slot = 1.
Connector COM2, Logical Line 1 time_slot = 2.
Connector COM2, Logical Line 1 time_slot = 3.
Connector COM2, Logical Line 1 time_slot = 4.
Connector COM2, Logical Line 1 time_slot = 5.
Connector COM2, Logical Line 1 time_slot = 6.
Connector COM2, Logical Line 1 time_slot = 7.
#   16: mm/dd/yy 10:31:33.234   DEBUG     SLOT  5  DS1E1    Code:  50
Connector COM2, Logical Line 1 time_slot = 8.
Connector COM2, Logical Line 1 time_slot = 9.
Connector COM2, Logical Line 1 time_slot = 10.
Connector COM2, Logical Line 1 time_slot = 11.
Connector COM2, Logical Line 1 time_slot = 12.
Connector COM2, Logical Line 1 time_slot = 13.
Connector COM2, Logical Line 1 time_slot = 14.
Connector COM2, Logical Line 1 time_slot = 15.
Connector COM2, Logical Line 1 time_slot = 16.
Connector COM2, Logical Line 1 time_slot = 17.
Connector COM2, Logical Line 1 time_slot = 18.
Connector COM2, Logical Line 1 time_slot = 19.
Connector COM2, Logical Line 1 time_slot = 20.
Connector COM2, Logical Line 1 time_slot = 21.
#   17: mm/dd/yy 10:31:33.238   DEBUG     SLOT  5  DS1E1    Code:  50
Connector COM2, Logical Line 1 time_slot = 22.
Connector COM2, Logical Line 1 time_slot = 23.
Connector COM2, Logical Line 1 time_slot = 24.
Connector COM2, Logical Line 1 initialization complete
    Environment address    - 30675250 Line record address    - 307326ac
```

```
    Hardware map address    - 3072f784 Initialization block    -
80006c00
    Receive descriptor ring - 80002600 Transmit descriptor ring -
80005200
#  18: mm/dd/yy 10:31:58.218   DEBUG    SLOT 5 PCAP    Code:  67
interface became local - line 10905102
intf gate spawned - line 10905102
wait_state - line 10905102
```

To disable the payload Loopback, from Line Tests, click on "FDL Disable
Payload." (FDL stands for Facility Data Link.) The loopback LED turns off on
Port 1 in Slot 4, and the log displays the following messages:

```
[3:1]$ log -fftwid
#   1: mm/dd/yy 10:38:29.007   INFO     SLOT 3 TI      Code:   3
Log cleared !
#   2: mm/dd/yy 10:38:39.239   INFO     SLOT 2 MIB     Code:   7
wfSnmp.3.0 set to 192.32.18.9
#   3: mm/dd/yy 10:38:39.297   INFO     SLOT 2 MIB     Code:   5
wfDs1E1ActionEntry.5.905102 set to 6
#   4: mm/dd/yy 10:38:39.312   INFO     SLOT 4 DS1E1   Code:  31
Connector COM1 Unscheduled FDL message received - type Payload Loopback
Deactivate.
#   5: mm/dd/yy 10:38:39.355   DEBUG    SLOT 4 DS1E1   Code:  50
Connector COM1, Logical Line 1 time_slot = 1.
#   6: mm/dd/yy 10:38:39.359   DEBUG    SLOT 4 DS1E1   Code:  50
Connector COM1, Logical Line 1 time_slot = 2.
Connector COM1, Logical Line 1 time_slot = 3.
Connector COM1, Logical Line 1 time_slot = 4.
Connector COM1, Logical Line 1 time_slot = 5.
Connector COM1, Logical Line 1 time_slot = 6.
Connector COM1, Logical Line 1 time_slot = 7.
Connector COM1, Logical Line 1 time_slot = 8.
Connector COM1, Logical Line 1 time_slot = 9.
Connector COM1, Logical Line 1 time_slot = 10.
Connector COM1, Logical Line 1 time_slot = 11.
Connector COM1, Logical Line 1 time_slot = 12.
Connector COM1, Logical Line 1 time_slot = 13.
Connector COM1, Logical Line 1 time_slot = 14.
Connector COM1, Logical Line 1 time_slot = 15.
#   7: mm/dd/yy 10:38:39.363   DEBUG    SLOT 4 DS1E1   Code:  50
Connector COM1, Logical Line 1 time_slot = 16.
Connector COM1, Logical Line 1 time_slot = 17.
Connector COM1, Logical Line 1 time_slot = 18.
Connector COM1, Logical Line 1 time_slot = 19.
Connector COM1, Logical Line 1 time_slot = 20.
Connector COM1, Logical Line 1 time_slot = 21.
Connector COM1, Logical Line 1 time_slot = 22.
```

```
Connector COM1, Logical Line 1 time_slot = 23.
Connector COM1, Logical Line 1 time_slot = 24.
Connector COM1, Logical Line 1 initialization complete
    Environment address    - 30ea8ba0 Line record address    - 30f30dc4
    Hardware map address   - 30f2da34 Initialization block    -
80006800
    Receive descriptor ring - 80001000 Transmit descriptor ring -
80003c00
#    8: mm/dd/yy 10:38:39.367   DEBUG     SLOT  4  PCAP     Code:  67
interface became local - line 10904101
intf gate spawned - line 10904101
#    9: mm/dd/yy 10:38:39.371   DEBUG     SLOT  4  PCAP     Code:  65
wait_state - line 10904101
#   10: mm/dd/yy 10:38:44.351   DEBUG     SLOT  5  DP       Code:  67
Missing Circuit Options record cct #3.
DP gate rcv'd LINE message for cct 3.
#   11: mm/dd/yy 10:38:44.355   DEBUG     SLOT  5  DP       Code:  23
Creating Circuit 3 soloist with line GH 0xb381
#   12: mm/dd/yy 10:38:44.355   DEBUG     SLOT  5  GAME     Code:  23
SOLO (0x00403): election opening 3c000000/3c000000 (3c000000)
vote=00000000
#   13: mm/dd/yy 10:38:44.386   DEBUG     SLOT  5  GAME     Code:  97
SOLO (0x00403): election WON 0x04000000 (repl=bc000009/3c000000)
SOLO (0x00403): election CLOSING 3c000000/3c000000 (3c000000)
vote=00000000
#   14: mm/dd/yy 10:38:44.390   INFO      SLOT  5  ARP      Code:   1
Service is up on circuit 3
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

If you access the Line Tests option and send the FDL Line Loop CI, IA, or IB types, the following messages appear:

```
#    3: mm/dd/yy 10:43:14.207   INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.5.905102 set to 1
#    4: mm/dd/yy 10:43:14.207   INFO      SLOT  5  DS1E1    Code:  22
```

```
Connector COM2, Logical Line 1 LLC service withdrawn.
#    5: mm/dd/yy 10:43:14.238   INFO      SLOT  4  DS1E1   Code:   27
Connector COM1 Unscheduled FDL message received - type Line Loopback
Activate.
```

If you click on the FDL Disable Line Loop option, the LED turns off and the following log messages appear:

```
#    3: mm/dd/yy 10:46:19.624   INFO      SLOT  2  MIB     Code:    5
wfDs1E1ActionEntry.5.905102 set to 6
#    4: mm/dd/yy 10:48:24.391   INFO      SLOT  2  MIB     Code:    7
wfSnmp.3.0 set to 0.0.0.0
#    5: mm/dd/yy 10:48:24.454   DEBUG     SLOT  2  SNMP    Code:   35
Agent cleared lock.
#    6: mm/dd/yy 10:49:10.786   INFO      SLOT  2  MIB     Code:    7
wfSnmp.3.0 set to 192.32.18.9
#    7: mm/dd/yy 10:49:10.849   INFO      SLOT  2  MIB     Code:    5
wfDs1E1ActionEntry.5.905102 set to 4
#    8: mm/dd/yy 10:49:10.867   INFO      SLOT  4  DS1E1   Code:   28
Connector COM1 Unscheduled FDL message received - type Line Loopback
Deactivate.
#    9: mm/dd/yy 10:49:10.910   DEBUG     SLOT  4  DS1E1   Code:   50
Connector COM1, Logical Line 1 time_slot = 1.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Line	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

The Loopback LED lights. The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

The same unscheduled message shown in Line 8 earlier applies to FDL Line Loop IA and IB.

If you click on FDL Disable ALL, the MIB entity disables all FDL line loops. It sends a "Universal Loopback Deactivate" message.

```
#   16: mm/dd/yy 10:58:54.840    INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.5.905102 set to 7
#   17: mm/dd/yy 10:58:54.871    INFO      SLOT  4  DS1E1    Code:   32
Connector COM1 Unscheduled FDL message received - type Universal
Loopback Deactivate.
```

If you click on Loop Up, the line goes into a loopback state. The only visible evidence of this state is that the loopback LED lights. The log shows the following:

```
#    2: mm/dd/yy 11:02:41.489    INFO      SLOT  2  MIB      Code:   7
wfSnmp.3.0 set to 192.32.18.9
#    3: mm/dd/yy 11:02:41.552    INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.4.905102 set to 1
#    4: mm/dd/yy 11:02:47.292    INFO      SLOT  4  DS1E1    Code:   22
Connector COM1, Logical Line 1 LLC service withdrawn.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Line	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

If you click on Loop Down, the MIB entity disables the Line loopback and the log shows the following:

```
[3:1]$ log -fftwid
#    2: mm/dd/yy 11:06:25.815    INFO      SLOT  2  MIB      Code:   7
wfSnmp.3.0 set to 192.32.18.9
#    3: mm/dd/yy 11:06:25.918    INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.4.905102 set to 2
#    4: mm/dd/yy 11:06:31.675    DEBUG     SLOT  4  DS1E1    Code:   50
Connector COM1, Logical Line 1 time_slot = 1.
Connector COM1, Logical Line 1 time_slot = 2.
```

```
        Connector COM1, Logical Line 1 time_slot = 3.
        Connector COM1, Logical Line 1 time_slot = 4.
        Connector COM1, Logical Line 1 time_slot = 5.
        Connector COM1, Logical Line 1 time_slot = 6.
        Connector COM1, Logical Line 1 time_slot = 7.
        Connector COM1, Logical Line 1 time_slot = 8.
        Connector COM1, Logical Line 1 time_slot = 9.
        Connector COM1, Logical Line 1 time_slot = 10.
        #    5: mm/dd/yy 11:06:31.679   DEBUG    SLOT  4  DS1E1   Code:   50
        Connector COM1, Logical Line 1 time_slot = 11.
        Connector COM1, Logical Line 1 time_slot = 12.
        Connector COM1, Logical Line 1 time_slot = 13.
        Connector COM1, Logical Line 1 time_slot = 14.
        Connector COM1, Logical Line 1 time_slot = 15.
        Connector COM1, Logical Line 1 time_slot = 16.
        Connector COM1, Logical Line 1 time_slot = 17.
        Connector COM1, Logical Line 1 time_slot = 18.
        Connector COM1, Logical Line 1 time_slot = 19.
        Connector COM1, Logical Line 1 time_slot = 20.
        Connector COM1, Logical Line 1 time_slot = 21.
        Connector COM1, Logical Line 1 time_slot = 22.
        Connector COM1, Logical Line 1 time_slot = 23.
        Connector COM1, Logical Line 1 time_slot = 24.
        #    6: mm/dd/yy 11:06:31.683   DEBUG    SLOT  4  DS1E1   Code:  39
        Connector COM1, Logical Line 1 initialization complete
           Environment address - 30 - ea7ba0 Line record address -30f30dc4
           Hardware map address - 30f2da34 Initialization block - 80006800
           Receive descriptor ring - 80001000 Transmit descriptor ring - 80003c00
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------

Slot  Conn  State  MTU   Loopback   Accept     BERT  Line  Line    FDL   FDL
                         State      Loopback   Mode  Type  Coding  Type  Addr

4     1     Up     1600  No Loop    Enabled    Off   ESF   B8ZS    ANSI  BY

5     2     Up     1600  No Loop    Enabled    Off   ESF   B8ZS    ANSI  BY


2 entries in table.
```

If you change the setting of the Line Type parameter from ESF (extended super
frame) to SF (super frame), the following messages appear:

```
[3:1]$ s wfDs1E1ConfigEntry.wfDs1E1ConfigLineType.904101 3;commit
[3:1]$ s wfDs1E1ConfigEntry.wfDs1E1ConfigLineType.905102 3;commit
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
[3:1]$ !
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

If you set the port line type to AMI (alternate mark inversion), the following messages appear:

```
#    7: mm/dd/yy 11:25:03.226   WARNING    SLOT  4  DS1E1   Code:  14
Connector COM1 Loss of signal failure.
#    8: mm/dd/yy 11:25:03.226   INFO       SLOT  4  DS1E1   Code:  22
Connector COM1, Logical Line 1 LLC service withdrawn.
#    9: mm/dd/yy 11:25:03.335   INFO       SLOT  4  DS1E1   Code:  24
Connector COM1 B8ZS code received on port configured for AMI.
#   10: mm/dd/yy 11:25:05.343   WARNING    SLOT  5  DS1E1   Code:  17
Connector COM2 Remote alarm indication failure.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
------------------
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	**Red Alarm**	1600	No Loop	Enabled	Off	ESF	**AMI**	**AT&T**	BY
5	2	**Red Alarm**	1600	No Loop	Enabled	Off	ESF	**AMI**	**AT&T**	BY

```
2 entries in table.
```

If you configure the primary clock source as the Port 2 loop and the secondary clock source as the Port 1 loop, both clocks fail, and the following messages appear in the log:

```
#   62: mm/dd/yy 10:44:50.734   WARNING   SLOT  3  DS1E1   Code:   14
Connector COM2 Loss of signal failure.
#   63: mm/dd/yy 10:44:50.734   INFO      SLOT  3  DS1E1   Code:   23
Primary and Sec clocks unoperational - Switching to Internal Clock
Source.
```

The following message appears if you mismatch the line coding. In this example, the line coding of one side is AMI and the other is B8ZS (binary eight zeros substitution).

```
#  234: mm/dd/yy 09:01:43.121   INFO      SLOT  2  DS1E1   Code:   24
Connector COM1 B8ZS code received on port configured for AMI.
```

If you set the Line Type to ESF, many messages indicate bipolar violations on the side configured for AMI.

```
Ti prompt>  show ds1e1 fdl ansi1
DS1E1 Facility Data Link (FDL) errors (first half) - ANSI-403 mode:
-----------------
 Slot  Conn  CRC     BPV     OOF     FE      ES
             Counts  Counts  Counts  Counts  Counts

 2     1     65535   964252  0       0       1675
```

Appendix B
Using the Technician Interface to Configure and Run Packet Capture

This appendix include the following sections:

Overview

Packet Capture allows you to examine packets passing through selected circuits on a Bay Networks router. It copies the packets from the circuits to a file in the router's memory. You can then open the file and view the packets in order to troubleshoot a problem.

The following routers and physical media services support Packet Capture:

- Routers: AN, ANH, AFN, ASN, ALN, FN, LN, CN, BLN, BLN-2, BCN

- Physical media services: CSMA/CD (Ethernet), synchronous, T1, E1, MCT1, Token Ring, FDDI, HSSI, ISDN

You can use Packet Capture to do the following:

- Copy all incoming packets, outgoing packets, or both.

- Filter and copy incoming packets, outgoing packets, or both.

- Filter incoming packets, outgoing packets, or both, and copy only selected contents of those packets.

You can terminate Packet Capture as follows:

- Enter a command to terminate it immediately.

- Configure it to terminate itself when the Packet Capture file fills.

- Configure it to terminate itself when it matches a portion of an incoming or outgoing packet to a hexadecimal number or character string that you specify.

After Packet Capture terminates, you can choose one of the following options to examine the file. To take advantage of the maximum number of features for viewing a file, select the first option in the list that identifies the tools that you have available.

- If a Network General Sniffer is available, use the Optivity Internetwork 6.1 Tap software, FTP, TFTP, or XMODEM to transfer a copy of the Packet Capture file from the router to a UNIX workstation or DOS PC. You can then use one of the following methods to convert the file for processing by a Network General Sniffer:

  — Use Tap to convert the file on a UNIX workstation.

  — Use the Packet Convert utility to convert the file on a Sun workstation or DOS PC.

  Save the converted file on a DOS-formatted diskette and insert the diskette in a Network General Sniffer for analysis.

  Using a Network General Sniffer to view a Packet Capture file allows you to view each packet in a readable format. If one is available, we recommend that you use it to read Packet Capture files. Refer to *Using Optivity Internetwork 6.1* for the Tap instructions, or to this appendix for the Packet Convert instructions, and refer to the Network General Sniffer manual to read the file.

- If Optivity Internetwork 6.1 or later is available, and you can use it to establish a remote connection to the router, use the Optivity Tap application to transfer a copy of the Packet Capture file from the router, and display the packets in hexadecimal, summary, or decoded formats.

The decoded format identifies each field in the packet and, where appropriate, displays its contents in English. It also allows you to search packets for character strings.

Optivity Tap displays each packet in a readable format without requiring a Network General Sniffer. Refer to *Using Optivity Internetwork 6.1* or later for instructions.

- If a local or out-of-band Technician Interface connection to the router is available, and you can decode the hexadecimal content of the packets yourself, use it to display the packets.

  The Technician Interface shows the following information about each packet:

  — The sequential number of the packet in the file

  — The date and time Packet Capture copied the packet

  — The media carrying the packet

  — The original size of the packet

  — The direction of the packet (received for incoming, or transmitted for outgoing)

  — The contents of the packet in hexadecimal format.

  The Technician Interface also allows you to

  — Identify the first packet you want to display by specifying its sequence number in the packet capture file.

  — Limit the number of packets displayed.

- If a DOS PC or Sun workstation can establish an FTP, TFTP, or XMODEM connection to the router to transfer a copy of the file, you can use the Packet Dump utility to display the packets in hexadecimal format.

  The Packet Dump utility shows the same information about each packet as the Technician Interface, but it does not provide options for specifying the packet by number or quantity.

Implementation Notes

Packet Capture copies packets received or transmitted as error-free. It does not copy packets containing errors.

Packet Capture saves the MAC addresses in native media format.

Packet Capture does not display Frame Check Sequence (FCS) fields.

Getting Started

This section describes how to start and stop Packet Capture and look at a Packet Capture file. The default parameter values allow Packet Capture to copy all incoming packets from the circuits you specify until you enter a command to terminate it. After learning the basic features of Packet Capture, you can then go to "Using Advanced Features" to customize Packet Capture.

The basic instructions for using Packet Capture include the following sections:

*   "Preparing Packet Capture to Run"
*   "Starting Packet Capture"
*   "Terminating Packet Capture"
*   "Using the Technician Interface to Display a Packet Capture File"
*   "Deleting a Packet Capture Instance"

Preparing Packet Capture to Run

The following sections provide the minimum number of instructions required to prepare Packet Capture to run:

*   "Assigning the Processors to Run Packet Capture"
*   "Creating an Instance of Packet Capture"
*   "Allocating Memory for the Packet Capture File"
*   "Specifying the Number of Bytes in Each Packet to Copy"
*   "Enabling Packet Capture"

Assigning the Processors to Run Packet Capture

To assign processors to run Packet Capture, you determine which slots in the router contain the circuits from which you want to copy packets. Then enter the following Technician Interface command to assign the processors:

set wfProtocols.26.0 *<slot_mask>***;commit**

26 represents the wfPktCaptureLoad attribute (parameter).

<slot_mask> is a hexadecimal number representing one or more slots containing circuits or channels from which you want to copy packets.

If you want Packet Capture to copy packets from circuits in a single I/O module, use the associated slot mask listed in Table B-1.

Table B-1.   Determining the Slot Mask

Slot No.	Slot Mask
1	0x80000000
2	0x40000000
3	0x20000000
4	0x10000000
5	0x08000000
6	0x04000000
8	0x01000000
9	0x00800000
10	0x00400000
11	0x00200000
12	0x00100000
13	0x00080000
14	0x00040000

Example

To load Packet Capture on Slot 2, enter

set wfProtocols.26.0 0x40000000;commit

If you want to copy packets from more than one circuit, and the circuits are on different I/O modules, add the hexadecimal values for the associated slots listed in Table B-1, and use the sum as the slot mask.

Example

Capture packets from the I/O modules inserted into Slots 3, 4, 8, and 10 as follows:

1. **Add the associated slot masks as follows:**

Slot 3	0x20000000
Slot 4	0x10000000
Slot 8	0x01000000
Slot 10	0x00400000
	0x31400000

2. **Enter the sum in the set command as follows:**

   set wfProtocols.26.0 0x31400000;commit

Creating an Instance of Packet Capture

To create a Packet Capture record associated with a circuit or channel from which you want to copy packets, you reference the circuit's line number. A line number is a unique number used to identify a circuit. Site Manager creates a line number each time you add a circuit to the router's configuration.

When you create a Packet Capture record, it creates a set of default parameter values associated with the line number and stores them in the MIB. The standard MIB term for this type of record is an "instance."

Refer to the instructions in the section that applies to you:

* "Creating an Instance for MCT1"

* "Creating an Instance for Other Media"

Creating an Instance for MCT1

MCT1 uses logical lines within a physical connector. Each MCT1 line number represents a logical line.

Get the number of the logical line from which you want to copy packets as follows:

1. **Enter the following Technician Interface command to display the base line number:**

   get wfDs1E1PortMapEntry.4._<slot>_**.**_<connector>_

   4 represents the wfDs1E1PortMapLineNumber attribute (parameter).

   ### *Example*

   Enter the following to get the base line number of Connector 1 on an MCT1 I/O module in Slot 2.

   get wfDs1E1PortMapEntry.4.2.1

   In this example, the response is

   ```
   902101
   ```

2. **Enter the following command to display the logical line number:**

   get wfLogicalLineEntry.7._<base_line_number>_**.**_<index>_

   7 represents the wfLogicalLineNumber attribute (parameter).

   _<base_line_number>_ is the response to the command you entered in Step 1.

   <index> is the position of the logical line on the circuit.

   ### *Example*

   Enter the following to get the number of Logical Line 1 from the example in Step 1:

   get wfLogicalLineEntry.7.902101.1

   In this example, the response is

   ```
   10902101
   ```

Enter the following command to create an instance:

set wfPktCaptureEntry.1._<line_no.>_ **1;commit**

The first **1** represents the wfPktCaptureDelete attribute.

_<line_no.>_ is the response to the command you entered in Step 2. To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

The second **1** represents the numeric code for "create."

Example

Enter the following command to create an instance for Logical Line 10902101:

set wfPktCaptureEntry.1.10902101 1;commit

Creating an Instance for Other Media

Create an instance as follows:

1. **Find the media in the following list and enter the associated Technician Interface command to get the number of the logical line from which you want to copy packets.**

➡️ **Note: Enter the upper-case and lower-case characters exactly as they appear in these instructions.**

- Bisynchronous

    get wfBisyncEntry.13.*<slot>***.***<connector>*

    13 represents the wfBisyncLineNumber attribute.

- Ethernet (CSMA/CD)

    get wfCSMACDEntry.38.*<slot>***.***<connector>*

    38 represents the wfCSMACDLineNumber attribute.

- Sync, T1, E1, or ISDN B Channel

    get wfSyncEntry.79.*<slot>***.***<connector>*

    79 represents the wfSyncLineNumber attribute.

- Token Ring

    get wfTokenRingEntry.66.*<slot>***.***<connector>*

    66 represents the wfTokenRingLineNumber attribute.

- FDDI

    get wfFddiEntry.44.*<slot>***.***<connector>*

    44 represents the wfFDDILineNumber attribute.

- HSSI

  get wfHssiEntry.60.*<slot>***.***<connector>*

  60 represents the wfHssiLineNumber attribute.

- ISDN B Channel

  get wfIsdnBriInterfaceEntry.8.*<slot>***.***<connector>*

  8 represents the wfIsdnBriLineNumber attribute.

Example 1

Enter the following to get the line number of a SYNC interface on Slot 2, Connector 1:

get wfSyncEntry.79.2.1

The response is

202101 for Sync

Example 2

Enter the following to get the line number of an FDDI interface:

get wfFddiEntry.44.2.1

The response is

602101

2. **Enter the following command to create an instance:**

   set wfPktCaptureEntry.1.*<line_no.>* **1;commit**

   The first **1** represents the wfPktCaptureDelete attribute.

   <line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

   The second **1** represents the numeric code for "create."

   ### *Example*

   Enter the following command to create an instance for Line Number 202101:

   set wfPktCaptureEntry.1.202101 1;commit

Allocating Memory for the Packet Capture File

You must allocate memory to store the Packet Capture file in order to capture packets. By default, the Packet Capture file uses 0 bytes of memory.

Allocate memory to the Packet Capture file as follows:

1. **Enter the following command to display the maximum number of contiguous bytes available:**

   get wfKernelEntry.6.<i><slot no.></i> <i><value></i>

   6 represents the wfKernelMemoryMaxSegFree attribute.

➡️ **Note:** *The allocation of memory varies. If the processors have memory restrictions, enter this command every fifteen seconds for two to three minutes and record each response.*

2. **Enter the following command to specify the size of the Packet Capture file stored in memory:**

   set wfPktCaptureEntry.8.<i><line_no.></i> <i><value></i>**;commit**

   8 represents the wfPktCaptureBufSize attribute.

   <i><line_no.></i> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

   <i><value></i> is any number of 1024-byte increments in the range 1 to the number of bytes of (available contiguous memory minus 200 KB)/1024.The value 1 represents 1024 bytes of memory allocated for the Packet Capture file. The value 2 represents 2048 bytes. To calculate the value, subtract 200 KB from the lowest number displayed in response to the **get** command you entered in Step 1. Divide this by 1024. The answer is the maximum value that we recommend that you enter. The less memory you allocate to Packet Capture, the lower the chance that the processor will reset because of a memory problem. However, you do need to allocate enough memory to store the packets you want to capture.

If less than 200 KB of free memory remains after Packet Capture starts, it sends a warning message to the log. If errors occur after you start Packet Capture, stop it and allocate less memory.

Specifying the Number of Bytes in Each Packet to Copy

You must specify the number of bytes in each packet to copy to the Packet Capture file. If you want to use a Network General Sniffer to read a Packet Capture file, you must set the size of the packets to a value the Sniffer supports. The Sniffer currently supports the following values: 32, 64, 128, 256, and 512; they correspond to the Bay Networks router settings 1, 2, 4, 8, or 16.

Enter the following command to specify the number of bytes in each packet to copy into the Packet Capture file:

set wfPktCaptureEntry.9.*<line_no.>* *<value>***;commit**

9 represents the wfPktCapturePktSize attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is any number of 32-byte increments in the range 1—144. The value 1 represents 32 bytes to be saved. The value 144 represents 4608 bytes to be saved.

Enabling Packet Capture

Enter the following Technician Interface command to enable the Packet Capture software:

set wfPktCaptureEntry.2.*<line_no.>* **1;commit**

2 represents the wfPktCaptureDisable attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

The **1** represents the numeric code for "enable."

Example

Enter the following command to enable Packet Capture software for Line Number 202101:

set wfPktCaptureEntry.2.202101 1;commit

Starting Packet Capture

Enter the following Technician Interface command to start Packet Capture:

set wfPktCaptureEntry.5.<line_no.> **1;commit**

5 represents the wfPktCaptureControl attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

1 represents the numeric code for "start."

Example

Enter the following command to start Packet Capture software for Line Number 202101:

set wfPktCaptureEntry.5.202101 1;commit

Go to the next section.

Terminating Packet Capture

You must terminate Packet Capture before you can display the packets. Enter the following Technician Interface command to terminate it:

set wfPktCaptureEntry.5.<line_no.> **2;commit**

5 represents the wfPktCaptureControl attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

2 represents the numeric code for "stop."

Example

Enter the following command to enable Packet Capture software for Line Number 202101:

set wfPktCaptureEntry.5.202101 2;commit

Go to the next section.

Using the Technician Interface to Display a Packet Capture File

Enter the following Technician Interface command to display a Packet Capture file stored in memory:

pktdump *<line_no.>* [**-s***<start>*] [**-c***<count>*]

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

[**-s***<start>*] and [**-c***<count>*] are optional.

<start> is the number of the packet in the file to be displayed first. If you do not specify one, the Technician Interface displays Packet No. 1 first.

<count> is the number of packets to display in sequential order. If you do not specify one, the Technician Interface displays all packets.

If the Packet Capture file does not contain packets, the following message appears:

```
No packets captured for linenumber <line_no.>
```

If the Packet Capture file contains packets, the contents of each packet appear as follows:

- The first line shows information Packet Capture recorded about the packet. It includes

  — The sequential number of the packet in the file

  — The date and time Packet Capture copied the packet

  — The media carrying the packet

  If the media is Sync, the name of the protocol on the Sync interface appears instead of the media.

  — The number of bytes in the packet

  — The direction of the packet: "Rx" for incoming packets and "Tx" for outgoing packets.

- The remaining lines show the data in the packet in hexadecimal format.

Example 1

Enter the following command to display all packets associated with Line Number 102101:

pktdump 102101

```
Pkt#   1 mm/dd/yy 10:20:26.430 CSMACD 60 Rx

00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42

00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 3f 09 ef df 00 00 01 00 00 00 00 00

Pkt#   2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx

00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01

00000010: 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00

Pkt#   3 mm/dd/yy 10:20:28.462 CSMACD 60 Rx

00000000: 00 00 a2 00 93 c5 00 00 a2 00 93 c5 81 02 01 01

00000010: 00 00 00 00 30 5b 00 00 00 00 00 00 00 00 00 00

00000020: a9 4b 16 aa e9 1d 00 00 00 00 a8 c0 00 00 00 00

00000030: 14 00 02 00 0f 00 b6 05 5a 51 0f 00 00 00 00 00
```

Example 2

Enter the following command to display all packets starting with Packet No. 2 in the Packet Capture file:

pktdump 102101 -s2

```
Pkt#   2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx

00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01

00000010: 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00
```

```
Pkt#   3 mm/dd/yy 10:20:28.462 CSMACD 60 Rx

00000000: 00 00 a2 00 93 c5 00 00 a2 00 93 c5 81 02 01 01

00000010: 00 00 00 00 30 5b 00 00 00 00 00 00 00 00 00 00

00000020: a9 4b 16 aa e9 1d 00 00 00 00 a8 c0 00 00 00 00

00000030: 14 00 02 00 0f 00 b6 05 5a 51 0f 00 00 00 00 00
```

Example 3

Enter the following command to display only the first packet in the Packet
Capture file:

pktdump 102101 -c1

```
Pkt#   1 mm/dd/yy 10:20:26.430 CSMACD 60 Rx

00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42

00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 3f 09 ef df 00 00 01 00 00 00 00 00
```

Example 4

Enter the following command to display only the second packet in the Packet
Capture file:

pktdump 102101 -s2 -c1

```
Pkt#   2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx

00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01

00000010: 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00
```

Deleting a Packet Capture Instance

You may want to delete all MIB information about a Packet Capture instance if you no longer intend to use it and you want to free the memory for other purposes. To delete an instance, enter the following command:

set wfPktCaptureEntry.1.<*line_no.*> **2;commit**

1 represents the wfPktCaptureDelete attribute.

<*line_no.*> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

2 represents the numeric code for "delete."

Example

Enter the following command to delete the Packet Capture instance identified by Line Number 202101:

set wfPktCaptureEntry.1.202101 2;commit

Using Optional Features

The following sections describe how to use optional Packet Capture features:

- "Configuring the Direction of the Packets to be Copied"

- "Configuring a Termination Trigger"

- "Assigning Filters"

- "Configuration Examples"

- "Configuring the Direction of the Packets to be Copied"

➡️ **Note:** *If Packet Capture is running and you change the configuration, the change will not affect Packet Capture until you stop it and restart it.*

Configuring the Direction of the Packets to be Copied

This section describes how to change the direction of the packets to be copied. By default, Packet Capture copies only incoming packets.

Enter the following command to change the direction of the packets that Packet Capture saves:

set wfPktCaptureEntry.10.<line_no.> <value>**;commit**

10 represents the wfPktCaptureDirection attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is one of the following:

•   1—Packet Capture will copy only incoming packets.

•   2—Packet Capture will copy only outgoing packets.

•   3—Packet Capture will copy both incoming and outgoing packets.

Example

Enter the following command to configure Packet Capture to copy both incoming and outgoing packets associated with Line Number 102101:

set wfPktCaptureEntry.10.102101 3;commit

Configuring a Termination Trigger

By default, Packet Capture terminates only when you issue the command to terminate it. You can change this default so that Packet Capture terminates

•   When the Packet Capture file fills.

•   Or when it matches a portion of an incoming or outgoing packet to a hexadecimal number or character string that you specify.

You can issue a command to terminate Packet Capture even if you configure it to terminate on its own.

If you want Packet Capture to terminate itself and

- You configured Packet Capture to copy incoming packets, enter

  set wfPktCaptureEntry.12.*<line_no.> <value>***;commit**

  12 represents the wfPktCaptureRxTrigger attribute.

- You configured Packet Capture to copy outgoing packets, enter

  set wfPktCaptureEntry.13.*<line_no.> <value>***;commit**

  13 represents the wfPktCaptureTxTrigger attribute.

Enter both commands if you want to change the trigger settings for both incoming and outgoing packets.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is one of the following:

- 1—Packet Capture terminates when the Packet Capture file fills. If the setting is not 1 and the file fills, Packet Capture writes over the oldest packets in the file.

Caution: *If you configure Packet Capture to copy both received and transmitted packets, it copies them to a single file. Therefore, if you choose both packet directions, and set one of these parameters (Receive Trigger or Transmit Trigger) to 1, you must set the other to 1. If you fail to do this, Packet Capture may write over the oldest packets, regardless of whether an interface received or transmitted them.*

- 2—Packet Capture terminates when data matches the value of the Filter 1 Match parameter for the packet direction queried.

- 3—Packet Capture terminates when data matches the value of the Filter 2 Match parameter for the packet direction queried.

- 4—Packet Capture runs until you terminate it manually. This is the default setting.

Example

Enter the following command if you configured the Packet Capture instance associated with Logical Line No. 102101 to copy only incoming packets and you want it to terminate itself when it matches packet data to the Filter 2 Match parameter:

set wfPktCaptureEntry.12.102101 3;commit

Assigning Filters

Use this section if you want to specify a string of alphanumeric characters to compare with the packet data.

When Packet Capture matches packet data to the string, it either copies the packet to the Packet Capture file or it terminates without copying the packet.

Packet Capture supports two filters for incoming packets and two filters for outgoing packets. The filter names are:

- Receive Filter 1 matches incoming packet data to a string you specify.

- Receive Filter 2 matches incoming packet data to a second string you specify.

- Transmit Filter 1 matches outgoing packet data to a string you specify.

- Transmit Filter 2 matches outgoing packet data to a second string you specify.

Each filter has its own set of parameters. They are as follows:

- Type — Determines whether Packet Capture terminates when it finds a match, copies a packet when it matches it to the string, or copies every packet on a circuit.

- Match — the hexadecimal number or string of characters that Packet Capture uses to compare to the data in a packet.

- Reference, Offset, and Size— the data within the packet to compare with the string. Reference identifies the field of the packet. Offset determines the number of bytes after the Reference with which to begin the comparison. Size determines the number of bytes to compare to the string.

Packet Capture also supports one Group parameter for each packet direction. The Group parameter allows you to specify whether the packet must match both Filter 1 and Filter 2 in order for Packet Capture to copy it.

Refer to the following sections to set the parameters for each filter.

➡️ **Note:** *To avoid confusion, configure all of the parameter settings of one filter before going to the next. For example, configure all of the Receive Filter 1 parameters before configuring the Receive Filter 2 parameters.*

Setting the Filter Response to a Match

Enter the following Technician Interface command to set the response to the filter:

set wfPktCaptureEntry.*<attribute_no.>***.***<line_no.>* *<value>***;commit**

<attribute_no.> is

- **14** for Receive Filter 1

  14 represents the wfPktCaptureRxFltr1Type attribute.

- **24** for Receive Filter 2

  24 represents the wfPktCaptureRxFltr2Type attribute.

- **19** for Transmit Filter 1

  19 represents the wfPktCaptureTxFltr1Type attribute.

- **30** for Transmit Filter 2

  30 represents the wfPktCaptureTxFltr2Type attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is

- 1 if you want Packet Capture to copy only the packets containing the data that matches the string.

- 2 if you want Packet Capture to terminate when it matches data in a packet to the string. Packet Capture does not copy the packet containing the match.

- 3 if you want Packet Capture to copy every packet on a circuit, regardless of its contents. If you use this setting, Packet Capture does not use the remaining parameter settings for the associated filter.

Note: *You can configure a filter as a capture type (1) or a trigger type (2), but not both. If you configure two receive filters, one a capture filter and the other a trigger filter, make Filter 2 the trigger filter.*

Specifying the String to Compare with the Packet Data

Enter the following Technician Interface command to create a string of characters to match with the packet:

set wfPktCaptureEntry.*<attribute_no.>***.***<line_no.>* *<value>***;commit**

<attribute_no.> is

- **18** for Receive Filter 1

  18 represents the wfPktCaptureRxFltr1Match attribute.

- **28** for Receive Filter 2

  28 represents the wfPktCaptureRxFltr2Match attribute.

- **23** for Transmit Filter 1

  23 represents the wfPktCaptureTxFltr1Match attribute.

- **34** for Transmit Filter 2

  34 represents the wfPktCaptureTxFltr2Match attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is any hexadecimal number or character string up to 16 characters.

Specifying the Data to Compare with the String

Refer to the following sections to specify the data within the packet to compare with the string:

- "Specifying the Reference"
- "Specifying the Offset"
- "Specifying the Number of Bytes"

Specifying the Reference

Enter the following Technician Interface command to specify the reference, which is the field in the packet:

set wfPktCaptureEntry.<attribute_no.>**.**<line_no.> <value>**;commit**

<attribute_no.> is

*   **16** for Receive Filter 1

    16 represents the wfPktCaptureRxFltr1Ref attribute.

*   **26** for Receive Filter 2

    26 represents the wfPktCaptureRxFltr2Ref attribute.

*   **21** for Transmit Filter 1

    21 represents the wfPktCaptureTxFltr1Ref attribute.

*   **32** for Transmit Filter 2

    32 represents the wfPktCaptureTxFltr2Ref attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is

*   1 for the first byte of the packet.

    Specify 1 if you want the copied portion of the packet to contain Media Access Control information.

*   2 for data link.

*   3 for multicast.

    Specify 3 if you want to use a special filter to make sure the right-most bit of a byte is a 1.

    To specify a multicast bit for Ethernet, specify 3. Then set the offset to 0.

    To specify a source routing bit for Token Ring, specify 3. Then set the offset to 6.

Specifying the Offset

Enter the following Technician Interface command to specify the number of bytes after the Reference with which to begin the comparison:

set wfPktCaptureEntry.*<attribute_no.>***.***<line_no.>* *<value>***;commit**

<attribute_no.> is

- **15** for Receive Filter 1

  15 represents the wfPktCaptureRxFltr1Offset attribute.

- **25** for Receive Filter 2

  25 represents the wfPktCaptureRxFltr2Offset attribute.

- **20** for Transmit Filter 1

  20 represents the wfPktCaptureTxFltr1Offset attribute.

- **31** for Transmit Filter 2

  31 represents the wfPktCaptureTxFltr2Offset attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is any number up to the number of bytes in the packet. Refer to the media you are filtering in the section "Media-Specific Instructions and Examples" later in this appendix for detailed instructions.

Specifying the Number of Bytes

Enter the following Technician Interface command to specify the number of bytes to compare with the string:

set wfPktCaptureEntry.*<attribute_no.>***.***<line_no.>* *<value>***;commit**

<attribute_no.> is

- **17** for Receive Filter 1

  17 represents the wfPktCaptureRxFltr1Size attribute.

- **27** for Receive Filter 2

  27 represents the wfPktCaptureRxFltr2Size attribute.

- **22** for Transmit Filter 1

  22 represents the wfPktCaptureTxFltr1Size attribute.

- **33** for Transmit Filter 2

  33 represents the wfPktCaptureTxFltr2Size attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> equals the number of characters in the Match parameter setting. It cannot exceed 16.

Selecting the Number of Filters that Must Match

Use this section if you did both of the following tasks:

- You configured both filters associated with a packet direction.
- You set the Type parameter for both filters to 1 to copy only packets that match the string.

Enter the following command to specify whether the packet must match both Filter 1 and Filter 2 in order for Packet Capture to copy it:

set wfPktCaptureEntry.*<attribute_no.>***.***<line_no.> <value>***;commit**

<attribute_no.> is

- **29** for Receive Filter 1 and Receive Filter 2

  29 represents the wfPktCaptureRxFltr2Group attribute.

- **35** for Transmit Filter 1 and Transmit Filter 2

  35 represents the wfPktCaptureTxFltr2Group attribute.

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

<value> is

- 1 if you want Packet Capture to copy a packet if it matches either Filter 1 or Filter 2.

- 2 if you want Packet Capture to copy a packet only if it matches both Filter 1 and Filter 2.

➡ **Note:** *Packet Capture uses this parameter only if you configure both capture filters associated with a single direction.*

Configuration Examples

This section shows examples of packet capture configurations. The circuit is on a CSMA/CD interface. The line number is 102101.

Example 1

This example sets the following configuration:

- 1024 bytes of memory reserved for Packet Capture

- 64 bytes of each packet to be saved

- Incoming and outgoing packets to be saved

- No filters and No triggers

The instructions are as follows:

1. **Reserve 1024 bytes of memory:**

   set wfPktCaptureEntry.8.102101 1

   8 represents the wfPktCaptureBufSize attribute.

2. **Save 64 bytes of each packet:**

   set wfPktCaptureEntry.9.102101 2

   9 represents the wfPktCapturePktSize attribute.

3. **Save incoming and outgoing packets:**

   set wfPktcaptureEntry.10.102101 3;commit

   10 represents the wfPktCaptureDirection attribute.

Example 2

This example starts and stops Packet Capture. The instructions are as follows:

1. **Start Packet Capture:**

   set wfPktCaptureEntry.5.102101 1;commit

   5 represents the **wfPktCaptureControl** attribute.

2. **Stop Packet Capture:**

   set wfPktCaptureEntry.5.102101 2;commit

Example 3

This example configures a termination trigger for each direction. The instructions are as follows:

1. **Set a trigger for incoming packets:**

   set wfPktCaptureEntry.12.102101 1

   12 represents the wfPktCaptureRxTrigger attribute.

2. **Set a trigger for outgoing packets:**

   set wfPktCaptureEntry.13.102101 1;commit

   13 represents the wfPktCaptureTxTrigger attribute.

Example 4

This example specifies that Packet Capture copy only incoming packets with a Type field containing the hexadecimal number 0800. The instructions are as follows:

1. **Copy only incoming packets that match the Receive Filter 1 Match parameter setting:**

   set wfPktCaptureEntry.14.102101 1

   14 represents the wfPktCaptureRxFltr1Type attribute.

2. **Specify the Reference with which to begin the comparison:**

   set wfPktCaptureEntry.16.102101 1

   16 represents the wfPktCaptureRxFltr1Ref attribute.

3. **Specify** the number of bytes after the Reference **with which to begin the comparison:**

   set wfPktCaptureEntry.15.102101 12

   15 represents the wfPktCaptureRxFltr1Offset attribute.

4. **Specify the number of bytes in the packet to compare with the string:**

   set wfPktCaptureEntry.17.102101 2

   17 represents the wfPktCaptureRxFltr1Size attribute.

5. **Specify the string as the hexadecimal number 0800:**

   set wfPktCaptureEntry.18.102101 0x0800;commit

   18 represents the wfPktCaptureRxFltr1Match attribute.

Example 5

This example specifies that Packet Capture copy only incoming packets with both a Type field of hexadecimal 0800 and a destination MAC address of ffffffffffff. It assumes you already specified the Type field as shown in <u>Example 4</u>. The instructions are as follows:

1. **Copy incoming packets that match the Receive Filter 2 Match parameter setting:**

   set wfPktCaptureEntry.24.102101 1

   24 represents the wfPktCaptureRxFltr2Type attribute.

2. **Specify the Reference with which to begin the comparison:**

   set wfPktCaptureEntry.26.102101 1

   26 represents the wfPktCaptureRxFltr2Ref attribute.

3. **Specify** the number of bytes after the Reference **with which to begin the comparison:**

   set wfPktCaptureEntry.25.102101 0

   25 represents the wfPktCaptureRxFltr2Offset attribute.

4. **Specify the number of bytes in the packet to compare with the string:**

   set wfPktCaptureEntry.27.102101 6

   27 represents the wfPktCaptureRxFltr2Size attribute.

5. **Specify the string as the hexadecimal number ffffffffffff:**

   set wfPktCaptureEntry.28.102101 0xffffffffffff

   28 represents the wfPktCaptureRxFltr2Match attribute.

6. **Specify that Packet Capture copy a packet only if it matches both the Receive Filter 1 Match and Receive Filter 2 Match parameter settings:**

   set wfPktCaptureEntry.29.102101 2;commit

   29 represents the wfPktCaptureRxFltr2Group attribute.

Displaying the Current Packet Capture Configuration Settings

Enter the following command to display the current Packet Capture configuration:

get wfPktCaptureEntry.*.<line_no.>

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

The Technician Interface displays a value for each attribute. Go to the "Reference Guide" section for a description of each attribute and its possible values.

Example

```
get wfPktCaptureEntry.*.102101
wfPktCaptureEntry.wfPktCaptureDelete.102101 = 1
wfPktCaptureEntry.wfPktCaptureDisable.102101 = 1
wfPktCaptureEntry.wfPktCaptureState.102101 = 1
wfPktCaptureEntry.wfPktCaptureFname.102101 = "PCAP0200"
wfPktCaptureEntry.wfPktCaptureControl.102101 = 1
wfPktCaptureEntry.wfPktCaptureCapture.102101 = 2
wfPktCaptureEntry.wfPktCaptureLineNumber.102101 = 102101
wfPktCaptureEntry.wfPktCaptureBufSize.102101 = 0
wfPktCaptureEntry.wfPktCapturePktSize.102101 = 0
wfPktCaptureEntry.wfPktCaptureDirection.102101 = 1
wfPktCaptureEntry.wfPktCaptureCount.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxTrigger.102101 = 4
wfPktCaptureEntry.wfPktCaptureTxTrigger.102101 = 4
wfPktCaptureEntry.wfPktCaptureRxFltr1Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureRxFltr1Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr1Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureRxFltr1Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr1Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureTxFltr1Type.102101 = 3
```

```
wfPktCaptureEntry.wfPktCaptureTxFltr1Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr1Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr1Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr1Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureRxFltr2Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureRxFltr2Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr2Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureRxFltr2Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr2Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureRxFltr2Group.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr2Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureTxFltr2Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr2Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr2Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr2Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureTxFltr2Group.102101 = 1
```

Displaying Event Messages Issued by Packet Capture

Enter the following Technician Interface command to display the Packet Capture event messages:

log -fftwid -ePCAP

Refer to *Event Messages for Routers and BNX Platforms* for information about the events.

Using a Sun Workstation or DOS PC to Display Packets

This section includes the following topics:

- "Getting the Name of the Packet Capture File"

- "Using FTP to Transfer the File"

- "Using TFTP to Transfer the File"

- "Using XMODEM to Transfer the File"

- "Displaying the File"

Getting the Name of the Packet Capture File

To get a Packet Capture file stored in the router's memory, you must know its name. Enter the following command to get the filename:

get wfPktCaptureEntry.4. *<line_no.>*

<line_no.> is the number displayed after you issued the **get** command in "Creating an Instance of Packet Capture." To list the current line numbers associated with Packet Capture, enter the **list instances wfPktCaptureEntry** command.

4 represents the wfPktCaptureFname attribute.

The filename displayed is in the following format:

PCAP*<ssnn>*

ss is the slot number.

nn is a number from 00 to 99

Example

Enter the following command to display the name of the captured packets associated with Line No. 102101:

get wfPktCaptureEntry.4.102101

Using FTP to Transfer the File

When you use FTP to get a Packet Capture file, the FTP software transfers it from the processor's memory instead of the media.

The procedure for using FTP to transfer a copy of a file to a Sun workstation or PC depends on the implementation of FTP on that system. The following instructions apply to Sun workstations. If you are using a PC and need instructions for using FTP, refer to the documentation for the TCP/IP stack installed on the PC.

Enter the following commands at the command line interface of the Sun workstation:

1. Issue the following command to start FTP:

   FTP

2. **Issue the following command to establish an FTP connection with the router.**

   open *<IP_address>*

   <IP_address> is the IP address of the router.

   Example

   connect 1.1.1.1

3. **Enter the following command to specify that the file to be transferred is binary:**

   mode binary

4. **Enter the following command to retrieve a copy of the file:**

   get *<filename>*

   <filename.> is the name displayed after you issued the **get** command in "Getting the Name of the Packet Capture File."

   Example

   get PCAP0400

5. **Enter the following command to terminate FTP:**

   quit

Using TFTP to Transfer the File

When you use TFTP to get a Packet Capture file, the TFTP software transfers it from the processor's memory instead of the media.

The procedure for using TFTP to transfer a copy of a file to a Sun workstation or PC depends on the implementation of TFTP on that system. The following instructions apply to Sun workstations. If you are using a PC and need instructions for using TFTP, refer to the documentation for the TCP/IP stack installed on the PC.

Enter the following commands at the command line interface of the Sun workstation:

1. **Issue the following command to start TFTP:**

   tftp

2. **Issue the following command to establish a TFTP connection with the router.**

connect *<IP_address>*

<IP_address> is the IP address of the router.

Example

connect 1.1.1.1

3. **Enter the following command to specify that the file to be transferred is binary:**

mode binary

4. **Enter the following command to retrieve a copy of the file:**

get *<filename>*

<filename.> is the name displayed after you issued the **get** command in "Getting the Name of the Packet Capture File."

Example

get PCAP0400

5. **Enter the following command to terminate TFTP:**

quit

Using XMODEM to Transfer the File

Enter the following Technician Inteface command to transfer a copy of the Packet Capture file from the router's memory:

xmodem sb *<filename>*

<filename> is the name displayed after you issued the **get** command in "Getting the Name of the Packet Capture File."

→ **Note:** *We support only single file mode for the XMODEM protocol. We do not support the YMODEM protocol.*

Displaying the File

You can use the Packet Dump utility to display a Packet Capture file that you retreived from the router.

The Site Manager installation software installs the Packet Dump utility on the following platforms:

- On DOS PCs, in the *\wf* directory. The filename is *pktdump.dos*.

- On SPARCstations, in the */usr/wf/bin* directory. The filename is *pktdump.spc*. The SPARCstation version runs only under SunOS.

These utilities are also available in the */perm/pkt_dump* directory on the Bay Networks FTP file server. Refer to Chapter 8 for file transfer instructions.

Access the directory and enter the following command at the Sun or DOS PC or UNIX command line:

pktdump *<filename>*

<filename> is the name of the Packet Capture file you retrieved from the router.

Packet Dump shows the same information about each packet as the Technician Interface, but it does not provide options for specifying the packet by number or quantity. Go to "Using the Technician Interface to Display a Packet Capture File" for a description of the fields and to "Example 1" within that section to look at a sample display.

Converting a Packet Capture File to Network General Sniffer Format

You can use the Packet Convert utility to a Packet Capture file that you retrieved from the router to Network General Sniffer format. This format allows the Sniffer to use the high level of decoding available to it to decode the captured packets.

The Site Manager installation software installs the Packet Convert utility on the following platforms:

- On DOS PCs, in the *\wf* directory. The filename is *pktconv.dos*.

- On SPARCstations, in the */usr/wf/bin* directory. The filename is *pktconv.spc*. The SPARCstation version runs only under SunOS.

These utilities are also available in the */perm/pkt_convert* directory on the Bay Networks FTP file server. Refer to Chapter 8 for file transfer instructions.

The Network General Sniffer reads MCT1 Packet Capture files as synchronous files.

You can convert HSSI packets only if the protocol is standard synchronous, such as PPP. You cannot convert packets if the protocol is HPTP protocol.

Packet Convert does not support the bisynchronous protocol.

➡ **Note:** You must set the size of the packets to one of the values the Sniffer supports before you capture them. Go to "Specifying the Number of Bytes in Each Packet to Copy" for instructions.

Convert a Packet Capture file as follows:

1. **Retrieve a copy of the file from the router.**

   Go to the following sections for instructions:

   — "Getting the Name of the Packet Capture File"

   — "Using FTP to Transfer the File," "Using TFTP to Transfer the File," or "Using XMODEM to Transfer the File"

2. **Make sure the filename does not have an extension and is nor more than 8 characters.**

3. **Access the directory containing the Packet Convert directory.**

4. **Enter the following command to convert the file:**

   pktconv *<filename>*

   Packet Capture creates a new file that you can copy to a DOS-formatted diskette and insert in the Sniffer. The name of the file begins with the Packet Capture filename and ends with the extension the Sniffer requires.

   Examples:

   • For a CSMA/CD Packet Capture file named *PCAP0400*, you enter

     pktconv pcap0400

     Packet Convert creates a Sniffer file named *PCAP0400.ENC*.

   • For a TOKEN Packet Capture file named *PCAP0300*, you enter

     pktconv pcap0300

Packet Convert creates a Sniffer file named *PCAP0300.TRC*.

- For a SYNC Packet Capture file named *PCAP0200*, you enter

  pktconv pcap0200

  Packet Convert creates a Sniffer file named *PCAP0200.SYC*.

- For a FDDI Packet Capture file named *PCAP0500*, you enter

  pktconv pcap0500

  Packet Convert creates a Sniffer file named *PCAP0500.FDC*.

➡️ **Note:** *If you use the Point to Point (Standard) protocol, the file will convert, but you must use the Sniffer Protocol Forcing option in order to decode the packets.*

Reference Guide to Packet Capture

This reference guide includes the following sections:

- "Displaying the Packet Capture Attribute Names and Numbers"
- "Packet Capture Parameter Descriptions"
- "Media-Specific Instructions and Examples"
- "Interpreting a Packet Capture Instance Number"

Displaying the Packet Capture Attribute Names and Numbers

Enter the following command to display the attributes of the Packet Capture (wfPktCaptureEntry) object and their associated numeric identifiers:

list wfPktCaptureEntry

➡️ **Note:** *Do not confuse the numeric identifier next to an attribute name with the value of that attribute. The numeric identifier is an alternative way to identify an attribute when issuing a* **get** *command. To get the values of the Packet Capture attributes, go to "Displaying the Current Packet Capture Configuration Settings" earlier in this appendix.*

Example

```
list wfPktCaptureEntry
wfPktCaptureDelete = 1
wfPktCaptureDisable = 2
wfPktCaptureState = 3
wfPktCaptureFname = 4
wfPktCaptureControl = 5
wfPktCaptureCapture = 6
wfPktCaptureLineNumber = 7
wfPktCaptureBufSize = 8
wfPktCapturePktSize = 9
wfPktCaptureDirection = 10
wfPktCaptureCount = 11
wfPktCaptureRxTrigger = 12
wfPktCaptureTxTrigger = 13
wfPktCaptureRxFltr1Type = 14
wfPktCaptureRxFltr1Offset = 15
wfPktCaptureRxFltr1Ref = 16
wfPktCaptureRxFltr1Size = 17
wfPktCaptureRxFltr1Match = 18
wfPktCaptureTxFltr1Type = 19
wfPktCaptureTxFltr1Offset = 20
wfPktCaptureTxFltr1Ref = 21
wfPktCaptureTxFltr1Size = 22
wfPktCaptureTxFltr1Match = 23
wfPktCaptureRxFltr2Type = 24
wfPktCaptureRxFltr2Offset = 25
wfPktCaptureRxFltr2Ref = 26
wfPktCaptureRxFltr2Size = 27
wfPktCaptureRxFltr2Match = 28
wfPktCaptureRxFltr2Group = 29
wfPktCaptureTxFltr2Type = 30
wfPktCaptureTxFltr2Offset = 31
wfPktCaptureTxFltr2Ref = 32
wfPktCaptureTxFltr2Size = 33
wfPktCaptureTxFltr2Match = 34
wfPktCaptureTxFltr2Group = 35
```

Packet Capture Parameter Descriptions

The following sections describe each parameter, its equivalent number, and its possible values:

- "Basic Parameters"

- "Trigger Parameters"

- "Filter Parameters"

➡️ **Note:** *Packet Capture reads attribute values only when it starts. To make Packet Capture respond to a change to an attribute value, stop it and restart it.*

If you configure an invalid value for an attribute, an error message appears in the log.

Basic Parameters

The basic parameters are common to all Packet Capture configurations. The basic parameters described in this section are as follows:

- Disable

- Delete

- Filename

- State

- Line Number

- Control

- Capture

- Packet Size

- Buffer Size

- Direction

- Count

Parameter:	**Delete**
Attribute Name:	wfPktCaptureDelete
Attribute Number:	1
Default:	1 (Create)
Options:	1 (Create)	2 (Delete)
Function:	The Create value reserves a memory location for a Packet Capture instance. Delete removes it.
Instructions:	Use the 1 setting to create the instance. Use the 2 setting to delete the instance if you do not plan to use it again in order to free the resources that Packet Capture uses.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.1
Parameter:	**Disable**
Attribute Name:	wfPktCaptureDisable
Attribute Number:	2
Default:	1 (Enable)
Options:	1 (Enable)	2 (Disable)
Function:	Controls the state of the Packet Capture instance.
Instructions:	Disabling an instance frees all resources allocated for the instance. If you had previously allocated a file stored in buffer memory, disabling the instance is an easy way to free the file stored in buffer memory and keep the MIB instance for future captures.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.2

Parameter:	**State**
Attribute Name:	wfPktCaptureState
Attribute Number:	3
Default:	1 (Up)
Options:	1 (Up)	2 (Down)	3 (Init)	4 (Not present)
	Up: An interface has registered and is enabled.
	Down: An interface has registered, but has been disabled.
	Init: Packet Capture is loaded on the slot, but there is no interface registered for this instance.
Function:	Not present: Packet Capture is not loaded on the slot that this instance is connected with. Indicates the state of the Packet Capture subsystem.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.3

Parameter:	**Filename**
Attribute Name:	wfPktCaptureFname
Attribute Number:	4
Default:	Set by Packet Capture code
Range:	PCAP<*ssnn*>
	ss is the slot number and *nn* is a number from 00 to 99.
Function:	Packet Capture sets this attribute, which contains the filename that can be used to retrieve the file stored in buffer memory for this instance.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.4

Parameter:	**Control**
Attribute Name:	wfPktCaptureControl
Attribute Number:	5
Default:	2 (Stop)
Options:	1 (Start)	2 (Stop)
	Start: Starts copying to a file. Stop: Terminates copying to a file.
Function:	Manually starts and stops a capture for this instance. You must stop Packet Capture before you can display the packets.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.5

Parameter:	**Capture**
Attribute Name:	wfPktCaptureCapture
Attribute Number:	6
Default:	2 (Stop)
Options:	1 (Start)	2 (Stop)
Function:	Indicates whether Packet Capture started or stopped.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.6

Parameter:	**Line Number**
Attribute Name:	wfPktCaptureLineLineNumber
Attribute Number:	7
Default:	Set by Packet Capture code.
Range:	Based on the encoded value.
Function:	Uniquely identifies a circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.7

Parameter:	**Buffer Size**
Attribute Name:	wfPktCaptureBufSize
Attribute Number:	8
Default:	None
Range:	1 (allocates 1024 bytes) | 2 (allocates 2048 bytes), … Available contiguous memory divided by 1024.
Function:	Sets the size of the file stored in buffer memory in 1024-byte increments. The upper limit is the maximum number of contiguous bytes of memory available on the slot. You can find the maximum number of contiguous bytes by entering
	get wfKernelEntry.6.<slot no.>
	6 represents the wfKernelMemoryMaxSegFree attribute.
Instructions:	If the allocation of the buffer leaves less than 200 KB of memory, a warning appears in the log. The operating system may need to allocate and free memory. If the memory needed is not available, an error occurs. If errors occur after you start Packet Capture, stop it and allocate a smaller buffer size.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.8

Parameter:	**Packet Size**
Attribute Name:	wfPktCapturePktSize
Attribute Number:	9
Default:	None
Range:	1 (32 bytes saved) | 2 (64 bytes saved), … 144 (4608 bytes saved)
Function:	Sets the number of bytes in 32-byte increments to be saved from a packet.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.9

Parameter:	**Direction**
Attribute Name:	wfPktCaptureDirection
Attribute Number:	10
Default:	1 (Receive)
Options:	1 (Receive)	2 (Transmit)	3 (Both)
Function:	Sets the direction of Packet Capture: copy received (incoming) packets, transmitted (outgoing) packets, or both.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.10

Parameter:	**Count**
Attribute Name:	wfPktCaptureCount
Attribute Number:	11
Default:	Set by the Packet Capture code.
Range:	Based on size of buffer and number of bytes saved.
Function:	Indicates the number of packets copied to the Packet Capture file.
Instructions:	If you use the default setting of the Trigger parameter and the capture buffer wraps, the count stops when it reaches a maximum value.
MIB Object ID:	1.3.6.1.4.1.18.3.4.21.1.1.11

Trigger Parameters

You use triggers to stop copying packets when an event occurs. The trigger parameters consist of a receive trigger and a transmit trigger. Each trigger stops Packet Capture, regardless of whether it is copying packets received, transmitted, or both.

The description of the Trigger parameters follows:

Parameters: **Trigger**

Packet Capture supports two trigger parameters. The MIB information is as follows:

Packet Direction	Attribute Name	Attribute No.	MIB Object ID
Incoming	wfPktCaptureRxTrigger	12	1.3.6.1.4.1.18.3.4.21.1.1.12
Outgoing	wfPktCaptureTxTrigger	13	1.3.6.1.4.1.18.3.4.21.1.1.13

Default: 4 (Not used)

Options: 1 (Buffer full) | 2 (Match Filter 1) | 3 (Match Filter 2) | 4 (Not used)

Function: Sets Packet Capture to terminate automatically when the packet data matches a string that you specify or when the Packet Capture file fills.

The Receive Trigger parameter terminates Packet Capture if you set it to a filter, and the incoming packet data matches a string that you specify.

The Transmit Trigger parameter terminates Packet Capture if you set it to a filter, and the outgoing packet data matches a string that you specify.

Instructions: If you want Packet Capture to terminate when the Packet Capture file fills, set the Receive and Transmit Triggers to 1. If you select an option other than 1 and the file fills, Packet Capture writes over the oldest packets in the file.

Caution: *If you configure Packet Capture to copy both incoming and outgoing packets, it copies them to a single file. Therefore, if you choose both packet directions, and set one of these parameters (Receive Trigger or Transmit Trigger) to 1, you must set the other parameter to 1. If you fail to do this, Packet Capture may write over the oldest packets, regardless of whether an interface received or transmitted them.*

If you want Packet Capture to terminate when it matches data to a string you specify, use one of the following options:

- 2 to terminate when data matches the Filter 1 Match parameter setting.

• 3 to terminate when data matches the Filter 2 Match parameter setting.

If you set the Packet Capture Receive Trigger to 2 or 3, it terminates upon matching data to either filter.

If you do not want Packet Capture to terminate automatically, use the default option (4).

Filter Parameters

The filter parameters described in this section are as follows:

• Type

• Offset

• Reference

• Size

• Match

• Group

Parameters: **Type**

Packet Capture supports four Type parameters. The MIB information is as follows:

Packet Direction	Filter No.	Attribute Name	Attribute No.	MIB Object ID
Incoming	1	wfPktCaptureRxFltr1Type	14	1.3.6.1.4.1.18.3.4.21.1.1.14
Incoming	2	wfPktCaptureRxFltr2Type	24	1.3.6.1.4.1.18.3.4.21.1.1.24
Outgoing	1	wfPktCaptureTxFltr1Type	19	1.3.6.1.4.1.18.3.4.21.1.1.19
Outgoing	2	wfPktCaptureTxFltr2Type	30	1.3.6.1.4.1.18.3.4.21.1.1.30

Default: 3 (Not used)

Options: 1 | 2 | 3

Function: Sets the filter type.

Instructions: Set to 1 (capture) if you want Packet Capture to copy only the packets containing the data that matches the string.

Set to 2 (trigger) if you want Packet Capture to terminate when it matches data in a packet to the string. Packet Capture does not copy the packet containing the match.

Set to 3 if you want Packet Capture to copy every packet on a circuit, regardless of its contents.

➡ **Note:** *You can configure a filter as a capture type or a trigger type, but not both. If you configure two receive filters, one a capture filter and the other a trigger filter, configure the trigger filter afterwards.*

Parameters: **Offset**

Packet Capture supports four Offset parameters. The MIB information is as follows:

Packet Direction	Filter No.	Attribute Name	Attribute No.	MIB Object ID
Incoming	1	wfPktCaptureRxFltr1Offset	15	1.3.6.1.4.1.18.3.4.21.1.1.15
Incoming	2	wfPktCaptureRxFltr2Offset	25	1.3.6.1.4.1.18.3.4.21.1.1.25
Outgoing	1	wfPktCaptureTxFltr1Offset	20	1.3.6.1.4.1.18.3.4.21.1.1.20
Outgoing	2	wfPktCaptureTxFltr2Offset	31	1.3.6.1.4.1.18.3.4.21.1.1.31

Default: None

Range: Limited to size of buffer.

Function: Sets the offset in bytes from the reference point into the packet. The byte pointed to by the offset is the first byte in the packet that will be checked for a match.

Instructions: Refer to the media you are filtering in the section "Media-Specific Instructions and Examples" later in this appendix.

Parameters: **Reference**

Packet Capture supports four Reference parameters. The MIB information is as follows:

Packet Direction	Filter No.	Attribute Name	Attribute No.	MIB Object ID
Incoming	1	wfPktCaptureRxFltr1Ref	16	1.3.6.1.4.1.18.3.4.21.1.1.16
Incoming	2	wfPktCaptureRxFltr2Ref	26	1.3.6.1.4.1.18.3.4.21.1.1.26
Outgoing	1	wfPktCaptureTxFltr1Ref	21	1.3.6.1.4.1.18.3.4.21.1.1.21
Outgoing	2	wfPktCaptureTxFltr2Ref	32	1.3.6.1.4.1.18.3.4.21.1.1.32

Default: 1

Options: 1 | 2 | 3

Function: Indicates the field in the packet to match.

Instructions: Set to one of the following:

- 1 for the first byte of the packet. Use this setting if you want the copied portion of the packet to contain Media Access Control information.

- 2 for data link.

- 3 for multicast.

Specify 3 if you want to use a special filter to make sure the right-most bit of a byte is a 1.

To specify a multicast bit for Ethernet, specify 3. Then set the offset to 0.

To specify a source routing bit for Token Ring, specify 3. Then set the offset to 6.

Parameters: **Size**

Packet Capture supports four Size parameters. The MIB information is as follows:

Packet Direction	Filter No.	Attribute Name	Attribute No.	MIB Object ID
Incoming	1	wfPktCaptureRxFltr1Size	17	1.3.6.1.4.1.18.3.4.21.1.1.17
Incoming	2	wfPktCaptureRxFltr2Size	27	1.3.6.1.4.1.18.3.4.21.1.1.27
Outgoing	1	wfPktCaptureTxFltr1Size	22	1.3.6.1.4.1.18.3.4.21.1.1.22
Outgoing	2	wfPktCaptureTxFltr2Size	33	1.3.6.1.4.1.18.3.4.21.1.1.33

Default: None

Range: Limited to 16 bytes

Function: Sets the length in bytes of the match field.

Instructions: Set the parameter in question to equal the number of characters in the Match parameter setting.

Parameters: **Match**

Packet Capture supports four Match parameters. The MIB information is as follows:

Packet Direction	Filter No.	Attribute Name	Attribute No.	MIB Object ID
Incoming	1	wfPktCaptureRxFltr1Match	18	1.3.6.1.4.1.18.3.4.21.1.1.18
Incoming	2	wfPktCaptureRxFltr2Match	28	1.3.6.1.4.1.18.3.4.21.1.1.28
Outgoing	1	wfPktCaptureTxFltr1Match	23	1.3.6.1.4.1.18.3.4.21.1.1.23
Outgoing	2	wfPktCaptureTxFltr2Match	34	1.3.6.1.4.1.18.3.4.21.1.1.34

Default: None

Range: Any hexadecimal number or character string

Function: Sets the hexadecimal number or character string to compare with the packet to test for a match.

Instructions: Enter any hexadecimal number or character string up to 16 characters.

Parameters: **Group**

Packet Capture supports two Group parameters: one for incoming packets and the other for outgoing packets. The MIB information is as follows:

Packet Direction	Attribute Name	Attribute No.	MIB Object ID
Incoming	wfPktCaptureRxFltr2Group	29	1.3.6.1.4.1.18.3.4.21.1.1.29
Outgoing	wfPktCaptureTxFltr2Group	35	1.3.6.1.4.1.18.3.4.21.1.1.35

Default: 1 (OR)

Options: 1 (OR) | 2 (AND)

Function: Determines whether Packet Capture copies a packet if it matches either filter or both filters. Packet Capture uses this parameter only if you configure both capture filters associated with a single direction.

Instructions: Use one of the following settings for each packet direction:

- 1 if you want Packet Capture to copy a packet if it matches either Filter 1 or Filter 2.

- 2 if you want Packet Capture to copy a packet only if it matches both Filter 1 and Filter 2.

Media-Specific Instructions and Examples

The following sections provide instructions and show examples of packets with different media types. They assume you set the number of bytes to copy from each packet to 64 by setting the wfPktCapturePktSize (wfPktCaptureEntry.9) to 2. Each example uses the **pktdump** command to show a hexadecimal decoding of a frame or packet.

CSMA/CD

The CSMA/CD (Ethernet) physical media has a data link filter offset of 14 bytes from the beginning of the MAC header. This places the data link filter point at the next byte after the TYPE/LENGTH field. Outgoing packets may contain less than 60 bytes each because they go to Packet Capture without padding.

An example of a hexadecimal display of a CSMA/CD frame follows.

```
Pkt# 10 mm/dd/yy 10:20:32.670 CSMACD 60 Rx

00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42

00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00

00000030: 02 00 0f 00 00 00 00 02 00 00 01 00 00 00 00 00
```

Protocols Supported By Synchronous, T1, E1, and MCT1

The following sections identify the format and filter offsets of the protocols supported by the synchronous, T1, E1, and MCT1 media, and show examples of these packets:

- "ATM"
- "Bisynchronous"
- "Frame Relay"
- "Frame Relay Switch and SMDS Switch"
- "LAPB"
- "Passthru"
- "PPP"
- "PTP (STANDARD)"
- "SDLC"
- "SMDS"
- "X.25"

ATM

The ATM protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an ATM packet follows:

```
Pkt# 20 04/23/94 09:57:29.968  ATM   548  Tx
00000000: 0c 80 00 85 00 4b 02 18 03 cc 45 00 02 14 01 10
00000010: 00 00 01 11 ed c9 64 00 00 01 64 ff ff ff 02 08
00000020: 02 08 02 00 69 c8 02 01 00 00 00 02 00 00 c0 20
00000030: de 00 00 00 00 00 00 00 00 00 00 00 00 02 00 02
```

Bisynchronous

The bisynchronous (BISYNC) protocol currently does not have a special data link filter. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works. The captured bisynchronous packets contain a 4-byte prefix that consists of internal information. This prefix is not present in the packets as they appear on the wire. The software uses the prefix to calculate an offset into the packet for filtering.

An example of a hexadecimal display of a bisynchronous packet follows:

```
Pkt#     1 01/01/94 03:17:56.284  BISYNC     9 Tx
00000000: 00 00 07 52 40 40 7f 7f 2d
```

Frame Relay

Frame relay does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a frame relay packet follows:

```
Pkt# 10 04/22/94 08:10:24.706 FR 45 Rx
00000000: 04 01 03 00 80 00 80 c2 00 0e 00 00 00 00 00 80
00000010: 00 00 00 a3 00 00 0c 00 00 00 00 80 00 00 00 a3
00000020: 00 00 0c 80 05 00 00 14 00 02 00 0f 00 9e 00 0e
```

Frame Relay Switch and SMDS Switch

The Frame Relay Switch and SMDS Switch work the same way as described in the "Frame Relay" and "SMDS" sections.

LAPB

The LAPB (Link Access Procedure-Balanced) protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a LAPB packet follows:

```
Pkt# 7 07/20/95 14:22:17.820 LAPB 5 Rx
```

00000000: 03 64 10 01 81

Passthru

The Passthru (PASS) protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a Passthru packet follows:

```
Pkt#   9 04/26/94 09:00:50.730 PASS 24 Tx
00000000: 07 03 00 00 a2 02 c9 b6 00 00 a2 02 c9 b6 81 02
00000010: 01 01 00 00 00 00 00 2a 00 00 00 00 00 00 00 00
```

PPP

The PPP (point-to-point; Standard Protocol) protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a PPP packet follows:

```
Pkt#   9 04/18/94 12:58:45.551 PPP 39 Rx
00000000: ff 03 02 01 00 00 00 00 00 80 00 00 00 a3 00 00
00000010: 0c 00 00 00 00 80 00 00 00 a3 00 00 0c 80 02 00
00000020: 00 14 00 02 00 0f 00 1d 00 00 00 00 00 00 00 00
```

PTP (STANDARD)

The PTP, or Standard, protocol has a data link filter offset of 16 bytes from the beginning of the packet. The data link filter is the first byte after the LENGTH/TYPE field.

Packet Capture receives the PTP packets without a reliable address field. This means that the packets marked Tx (for "transmit") have an accurate address field, but the packets marked Rx (for "receive") do not have an accurate address field.

An example of a hexadecimal display of a PTP packet follows:

```
Pkt#   9 04/22/94 08:07:52.812 PTP 54 Rx

00000000: 03 03 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26

00000010: 42 42 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c

00000020: 00 00 00 00 80 00 00 00 a3 00 00 0c 80 01 00 00

00000030: 14 00 02 00 0f 00 6b 0d 00 00 00 00 00 00 00 00
```

SDLC

The SDLC protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an SDLC packet follows:

```
Pkt# 1 07/20/95 14:45:27.910 SDLC 2 Tx
```

00000000: d1 bf

SMDS

The SMDS protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an SMDS packet follows:

```
Pkt# 10 04/22/94 08:09:20.211 SMDS 88 Rx

00000000: 05 03 00 00 00 87 00 4c e1 58 07 97 12 12 ff ff

00000010: c1 58 07 97 54 36 ff ff 05 03 00 00 03 00 01 00
```

```
00000020: 00 00 00 00 00 00 00 00 aa aa 03 00 80 c2 00 0e

00000030: 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00 00
```

X.25

The X.25 protocol currently does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works. The X.25 protocol uses the hardware's link layer capabilities. This means that Packet Capture receives only the frame's Layer 3 (packet layer) data.

An example of a hexadecimal display of an X.25 packet follows:

```
Pkt#   8 04/26/94 09:00:42.103 X25 47 Rx

00000000: 10 01 e2 00 00 00 00 00 01 00 00 00 00 00 02 00

00000010: 1e aa aa 03 00 00 a2 80 ff 00 00 a2 02 c9 b6 00

00000020: 00 a2 02 c9 b6 81 02 01 01 00 00 00 00 00 38 10
```

Token Ring

The Token Ring physical media has a data link filter offset of 14 bytes plus the RIF (routing information field) field, if a RIF is present. This places the data link filter point at the DSAP (destination service access point) byte. Packet Capture receives only LLC frames from the Token Ring. It does not receive the Access Control and Frame Control bytes at the beginning of each packet. Packet Capture inserts the hexadecimal value 1040 at the beginning of each packet for compatibility and possible future use.

An example of a hexadecimal display of a Token Ring frame follows:

```
Pkt# 10 04/18/94 12:58:58.885 TOKEN 52 Rx

00000000: 10 40 c0 00 00 00 01 00 00 00 c5 00 00 30 42 42

00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00

00000020: 00 00 80 00 00 00 a3 00 00 0c 80 06 00 00 14 00

00000030: 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00
```

FDDI

The FDDI physical media has a data link filter offset of 13 bytes. This places the data link filter point at the DSAP byte. Packet Capture does not receive all frames from the FDDI because the hardware handles some frames.

An example of a hexadecimal display of an FDDI frame follows:

```
Pkt# 10 04/18/94 12:59:04.017 FDDI 51 Rx
00000000: 50 80 01 43 00 00 00 00 00 c5 00 00 30 42 42 03
00000010: 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00 00
00000020: 00 80 00 00 00 a3 00 00 0c 80 08 00 00 14 00 02
00000030: 00 0f 00 b7 00 00 00 00 00 00 00 00 00 00 00 00
```

HSSI

The HSSI physical media works exactly the same way as the previously described SYNC medium, except for the HPTP (STANDARD) protocol.

HPTP has a data link filter offset of 14 bytes from the beginning of the packet. This places the data link filter point at the first byte after the Length/Type field. The HPTP packets do not have an address or control field.

An example of a hexadecimal display of an HSSI frame follows:

```
Pkt# 7 04/21/94 09:17:53.957 HPTP 52 Rx
00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 01 00 00 14 00
00000030: 02 00 0f 00 6b 0d 00 00 00 00 00 00 00 00 00 00
```

ISDN

The ISDN B Channel works the same way as described in the SYNC section for each of the protocols supported over ISDN.

The ISDN D Channel currently does not have a special data link offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an ISDN frame follows:

```
Pkt# 1 11/02/94 16:04:06.151  LAPD   26  Tx

00000000: 00 ad 00 00 08 01 01 05 a1 04 02 88 90 18 01 83

00000010: 70 08 80 32 32 34 30 33 38 37
```

Interpreting a Packet Capture Instance Number

When you create an instance of Packet Capture, you refer to the MIB to get the numeric identifier, called a line number, of the datapath channel. You then copy the line number when creating the Packet Capture instance. The instructions are in "Creating an Instance of Packet Capture" earlier in this appendix.

Site Manager automatically creates the line numbers when you use it to create a configuration file. A line number is a 10-digit, decimal number that is unique for each datapath channel in a router. Table B-2 shows the structure of a line number or Packet Capture instance number. The top row in the table is for the most significant digit and the bottom row is for the least significant digits. An example follows.

Table B-2.   Structure of a Line Number

Field	No. of Digits Reserved in the Field	Description
rsvd	1	Reserved and set to zero
chan	2	Line index for devices that use multiple lines per channel (zero for most boards)
type	2	The physical media type, which is one of the following: 1 for CSMACD 2 for synchronous 3 for T1 4 for E1 5 for TOKEN 6 for FDDI 7 for HSSI 9 for MCT1 13 for ISDN D Channel 15 for bisynchronous
slot	2	Number of the slot

(continued)

Table B-2.   Structure of a Line Number (continued)

Field	No. of Digits Reserved in the Field	Description
mod	1	Module number. On the ASN, the module number is in the range 1—4. All other platforms require that you set it to 1.
conn	2	Connector number for the specific medium

Example

The code for a single CSMA/CD interface on Slot 2 using XCVR1 is 0000102101. Site Manager removes the leading zeros, assigning a line number of 102101

Index

Symbols

boot
   failure, 3-3
   image. *See* router software image
   PROMs, 3-6

bouncing MAC addresses, 6-11

bridge ID, 6-4

buffers
   allocating for Packet Capture, B-10
   problem, 3-12

C

cables, 4-4

call request number, 6-23

cannot find file message, 7-2

carrier loss, 5-8

case-sensitivity, 1-17

cells, 5-2

Chameleon, 7-2

CHAP (Challenge Handshake Authentication
          Protocol), 6-29

check sequence (checksum) error, 5-8

checksum error, 5-8

circuit breaker, 3-2

circuit down, 5-14

clearlog command, 1-5

clipped frames, 5-10

clock settings, internal, 5-23

clock speed does not match other ports event
          message, 5-23

clocking, MCT1, 5-18

CN circuit breaker, 3-2

commands
   arp -a, 7-8
   backplane, 7-6
   clearlog, 1-5
   commit, 1-3, 1-16
   diags, 3-20
   get, 1-16, 8-3

get command wildcard character (*), 1-17
ifconfig -a, 7-8
list, 1-14 to 1-18
loadmap, 3-13 to 3-16
log, 1-7
monitor, 1-19
netstat -r, 6-8
osidata, 6-21
ping, 1-20
pktconv, B-34
pktdump, B-13, B-33
prom command failed, 1-4
put, 8-3
run setpath, 1-19
save config, 1-3
save log, 1-5
set, 1-2, 1-3, 1-16
show, 1-19
wfchkenv, 7-3
wfchkinst, 7-3

commit command, 1-2, 1-3, 1-16

communities, SNMP, 7-5

CompuServe, Bay Networks forum on, xvi

configuration files, consistency among slots, 3-9

Configuration Manager modes, 1-2

configuration, saving, 1-17

contiguous free space, 3-11

converting Packet Capture files, B-33

create attribute, 6-30

creation of a gate, 1-9

crossover cables, 5-23

CSMACD. *See* Ethernet

Current Screens List window, 1-20

customer support. *See* getting help

D

date and time, filtering events, 1-7

debug event messages, 1-7, A-1 to A-35

default zone – seed conflict event message, 6-3

G

GAME (Gate Access Management Entity), 1-9

gates, 1-9

get command, 1-16, 1-17

get command, 8-3

getting help
   from a Bay Networks Technical Response
      Center, xvii
   through CompuServe, xvi
   through InfoFACTS service, xvii
   through World Wide Web, xvii

GFWD (GAME forward) message type, A-5

global
   memory, 3-12
   parameters, 1-2
   source-route bridge settings, 6-4

group LAN ID, 6-4

group mode, 5-2, 5-16

GRPC (GAME remote procedure call) message
      type, A-5

H

heartbeat test, 5-10

help from the Bay Networks Technical Response
      Center, 8-1 to 8-3

host did not respond message, 6-12

HOST/ARP cache, 6-11

hot-swapping
   and fuses, 3-2
   cable support for, 4-4

HPTP, Packet Capture, B-34

HSSI
   Packet Capture, B-9, B-34, B-54

hybrid mode, 5-2

I

ICMP echo requests, 7-7

ifconfig -a command, 7-8

image names. *See* router software image names
      or boot PROMs

inbound Telnet. *See* Telnet

index of a logical line, B-7

InfoFACTS service, xvii

informational events, 1-7

instance, 1-10 to 1-18
   creating for Packet Capture, B-6
   deleting for Packet Capture, B-16
   format, 1-15

interface definition, 7-8

interframe time fill, 5-18

internal clock settings, 5-23

internal clocking, MCT1, 5-18

internal LAN ID, 6-4

internal overrun errors, 5-11

invalid ID, can't parse cmd line message, 6-22

invalid slot number, can't parse cmd line
      message, 6-22

IP, 6-6 to 6-16

IP addresses, UNIX, 7-8

IPX, 6-16 to 6-20

ISDN B Channel, Packet Capture, B-8, B-9, B-54

ISDN BRI and PRI, 6-27 to 6-29

K

killing a gate, 1-9

L

lack of resource, 5-8, 5-12

LAN ID, 6-4

LAPB (Link Access Procedure-Balanced), Packet
      Capture, B-51

late collisions, 5-11

Launch Facility tool, 1-20

X

Y

Z